BiPAC 7300NX/N *RE*

(3G) / Wireless-N
ADSL2+ Firewall Router

User Manual

Version Released: 1.05 (FW: v2.02b-dj1)

Last Revised on May 24, 2011

Table of Contents

Chapter 1 1
1.1 Introducing the BiPAC 7300NX/N *RE* 1
1.2 Features 3
1.3 Hardware Specifications 8
1.2 Applications of the devices 9
Chapter 2 11
2.1 Important Notes 11
2.2 Package Contents 12
2.3 The Front LEDs 13
2.4 The Rear Ports 14
BiPAC 7300N *RE* 14
BiPAC 7300NX 15
2.5 Cabling 17
Chapter 3 18
3.1 Before Configuration 18
3.2 Network Configuration 19
3.2.1 Configuring a PC in Windows 7 19
3.2.2 Configuring a PC in Windows Vista 21
3.2.3 Configuring a PC in Windows XP 23
3.2.4 Configuring a PC in Windows 2000 24
3.2.5 Configuring PC in Windows 98/Me 25
3.2.6 Configuring PC in Windows NT4.0 26
3.3 Factory Default Settings 27
3.4 LAN and WAN Port Addresses 28
3.5 Information from your ISP 28
3.6 Configuring with your BiPAC 7300NX/N *RE* 29
Chapter 4 33
4.1 Status 34
4.2 Quick Start 35
4.3 WAN 36
4.4 WLAN 39
Chapter 5 45
5.1 Status 46
5.1.1 ADSL Status 48
5.1.2 3G Status (BiPAC 7300NX only) 49
5.1.3 ARP Table 50
5.1.4 DHCP Table 50
5.1.5 System Log 51
5.1.6 Firewall Log 52
5.1.7 UPnP Portmap 53
5.2 Quick Start 54
5.3 Configuration 63
5.3.1 LAN (Local Area Network) 63
5.3.1.1 Ethernet 63
5.3.1.2 IP Alias 64

5.3.1.3 Wireless 65
5.3.1.4 Wireless Security 68
5.3.1.5 WPS 72
5.3.1.6 DHCP Server 85
5.3.2 WAN (Wide Area Network) 87
5.3.2.1 WAN Interface (BiPAC 7300NX only) 88
5.3.2.2 WAN Profile 90
5.3.2.3 ADSL Mode 101
5.3.3 System 102
5.3.3.1 Time Zone 103
5.3.3.2 Firmware Upgrade 104
5.3.3.3 Backup / Restore 105
5.3.3.4 Restart Router 106
5.3.3.5 User Management 106
5.3.3.6 Mail Alert 107
5.3.4 USB 109
5.3.4.1 User Management 109
5.3.4.2 Storage 112
5.3.4.3 Samba Server 115
5.3.4.4 FTP Server 116
5.3.5 Firewall 117
5.3.5.1 Packet Filter 119
5.3.4.2 MAC Filter 121
5.3.4.3 Intrusion Detection 122
5.3.4.4 Block WAN PING 124
5.3.4.5 URL Filter 124
5.3.5 QoS (Quality of Service) 127
5.3.6 Virtual Server 133
5.3.6.1 Port Mapping 135
5.3.6.2 DMZ 137
5.3.6.3 ALG 138
5.3.7 Wake on LAN 139
5.3.8 Time Schedule 140
5.3.9 Advanced 141
5.3.9.1 Static Route 142
5.3.9.2 Static ARP 142
5.3.9.3 Dynamic DNS 143
5.3.9.4 VLAN 144
5.3.9.5 Device Management 145
5.3.9.6 IGMP 152
5.3.9.7 SNMP Access Control 152
5.3.9.8 TR-069 client 155
5.3.9.9 Remote Access 156
5.4 Save Configuration to Flash 157
5.5 Restart 157
5.6 Logout 158
Chapter 6 159
Problems starting up the router 159
Problems with the WAN Interface 159
Problems with the LAN Interface 160

APPENDIX..... 161

Chapter 1
Introduction

1.1 Introducing the BiPAC 7300NX/N *RE*

The BiPAC 7300NX/N *RE* is an economical ADSL2+ router ideal for residential users to have an improved wireless access with a maximum operational speed of 300Mbps. It delivers the highest level of security with higher speed and better coverage of wireless-N solutions. The BiPAC 7300NX/N *RE* has integrated firewall security, providing protection for your valuable but vulnerable data and network against potential hack attacks and at the same time provides Quality of Service function, helping to prioritize queues of data traffic and ensure a smooth Internet connection. With two antennas, the BiPAC 7300NX/N *RE* is able to search for wireless signals inherently and intuitively**,** effectively reaching optimal connectivity**,** you can surf the Internet with the convenience and fun of mobility from every corner of your home or office. This device allows you to enjoy all Internet applications like music downloads, online gaming, video streaming, and file sharing with your family or colleagues! The BiPAC 7300NX router can even function as a FTP server for network device sharing.

High speed Access

Complying with worldwide ADSL standards, the BiPAC 7300NX/N *RE* supports downstream data transmission rates up to 12/24 Mbps with ADSL2/2+, 8 Mbps with ADSL, and performs at upstream rates of up to 1 Mbps. The BiPAC 7300NX/N *RE* includes Annex M technology that supports the latest ADSL2/2+ standard for higher upload speeds by increasing the upstream operation rate to approximately 2.5Mbps (up to 3Mbps under ideal conditions). With a Wireless-N Access Point that supports up to 300Mbps wireless operation rate, the BiPAC 7300NX/N *RE* is truly an enhanced Wireless LAN solution compared to the 802.11g standard. With all these technologies, users can enjoy high-speed access for broadband multimedia applications such as interactive gaming, video streaming and real-time audios that run faster and easier than ever.

Multiple Options for Internet Access

BiPAC 7300NX offers its USB port for connecting to a 3G / HSDPA USB modem, enabling you to use a 3G / HSDPA, UMTS, EDGE, GPRS, or GSM Internet connection, which makes downstream rates of up to 14.4 Mbps possible. Aiming for convenient and constant internet access for event or meeting organizers - allowing you to watch movies, download music on the road, or access e-mail no matter where you are. The **auto fail-over** feature ensures maximum connectivity and minimum interruption by quickly and smoothly connecting to a 3G network in the event once your ADSL line fails. This feature allows 7300NX automatically reconnect to the ADSL connection when it's restored, reducing connection costs.

BiPAC 7300N *RE* also equips its port #1 can be configured as a WAN port for connecting to ADSL, Cable, VDSL or a Fiber modem device, providing more options for users to access the Internet. So SOHO or small office users can even deploy the BiPAC 7300N *RE* for FTTx (Fiber-to-the-building, node, or home) applications over a VDSL or Fiber device connection.

State-of-the-art Security

Wi-Fi Protected Access (WPA-PSK / WPA2-PSK) and Wired Equivalent Privacy (WEP) features enhance the level of transmission security and access control over your Wireless LAN. The NAT default firewall has an advanced anti-hacker pattern-filtering protection features that can automatically detect and block Denial of Service (DoS) attacks. In addition, Packet Filtering provides high-level security for access control. Built with Stateful Packet Inspection (SPI), the router enables users to determine whether a data packet is allowed to pass through the firewall to the private LAN.

Ease of Set up and Management

Easy Sign-ON (EZSO), WPS push button and Auto-scan ADSL settings allow users to manage the device functions with minimum effort. The user-friendly, web-based user interface makes installing and managing the BiPAC 7300NX/N *RE* extremely easy. With support for both DHCP client and server, system administrators can manage IP assignment without having to reconfigure other stations and fitting the router into existing network environments.

1.2 Features

- Dual-WAN approach – ADSL2+ and 3G connections (BiPAC 7300NX only)
- Dual-WAN approach –ADSL2+ and Ethernet WAN for Broadband Connectivity (BiPAC 7300N *RE* only)
- USB 2.0 port for plugging a 3G / HSDPA modem as backup (available from your service provider) (BiPAC 7300NX only)
- Storage feature through USB 2.0 port: FTP Server, Samba server (BiPAC 7300NX only)
- 1x USB 2.0 port for multiple functions: 3G network, FTP server and Samba server (BiPAC 7300NX only)
- Auto fail-over feature to ensure an always-on connection (BiPAC 7300NX only)
- High-speed wireless connection up to 300Mbps
- Wireless-N Access Point with Wi-Fi Protected Setup (WPS), Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- Wireless On/Off time schedule control
- High speed Internet access with ADSL2/2+; also compatible with ADSL
- Integrated with 4-port Ethernet switch, for 7300N *RE*, port #1 can be configred as WAN port to connecting to ADSL/Cable/VDSL/ Fiber modem device
- SOHO firewall security with DoS prevention and SPI
- Universal Plug and Play (UPnP) Compliant
- Supports Virtual Private Network (VPN) pass-through
- Quality of Service Control
- Dynamic Domain Name System (DDNS)
- Easy Sign-ON (EZSO)
- Supports IPTV application[*5]

ADSL Compliance[*1]

- Compliant with ADSL Standards
  - Full-rate ANSI T1.413 Issue 2
  - G.dmt (ITU G.992.1)
  - G.lite (ITU G.992.2)
  - G.hs (ITU G.994.1)
  - ADSL over ISDN/U-R2

- Compliant with ADSL2 Standards
  - G.dmt.bis (ITU G.992.3)
  - ADSL2 Annex M (ITU G.992.3 Annex M) (available for BiPAC 7300NX/ N *RE A* model only)

- Compliant with ADSL2+ Standards
  - G.dmt.bis plus (ITU G.992.5)
  - ADSL2+ Annex M (ITU G.992.5 Annex M)(available for BiPAC 7300NX/ N *RE A* model only)

Network Protocols and Feathers

- NAT, static routing and RIP-1/2
- Universal Plug and Play (UPnP) Compliant
- Transparent Bridging
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS relay and IGMP proxy
- IGMP snooping for video service
- Management based-on IP protocol, port number and address
- SMTP Client

Firewall & Virtual Private Network(VPN)

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack and Ping of Death, etc.
- Remose access control for web base access
- Anti probe function
- Packet filtering, MAC filtering, URL content filtering
- Password protection for system management
- VPN pass-through

Qulity of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and address

IPTV Applications[*5]

- GMP Snooping
- Virtual LAN (VLAN)
- Quality of Services (QoS)
- IGMP Snooping & IGMP Proxy

Wireless LAN

- Compatible with IEEE 802.11n, IEEE 802.11g, 802.11b standards.
- Up to 300Mbps wireless operation rate [*2]
- 2.4 GHz–2.484 GHz frequency range
- WPS (Wi-Fi Protected Setup)
- 64/128 bits WEP supported for encryption
- Wireless Security with WPA-PSK/ WPA2-PSK support
- 802.1x radius supported
- WDS repeater function support

- WLAN on/off time schedule control

ATM and PPP Protocols

- ATM Adaptation Layer Type 5 (AAL5)
- Multiple Protocol over AAL5 (RFC 2684, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- MAC Encapsulated Routing (RFC 1483 MER)
- OAM F4/F5

USB Application Server(BiPAC 7300NX only)

- 3G network sharing
- Storage: FTP server, samba server

Management

- Easy Sign-ON (EZSO) and Auto-scan ADSL settings
- Web-based GUI for remote and local management
- Firmware upgrades and configuration data transfer via web-based interface
- Embedded Telnet server for remote and local management
- TR-069 *4 supports remote Management
- Available syslog
- Supports DHCP server/client/relay
- SNMP v1/v2/v3, MIB supported
- Wake on LAN
- Mail Alert for WAN IP changed, IDS, Failover/Failback management

Compatible 3G USB modems[*3] (BiPAC 7300NX only)

3G Brand	3G Model
ONDA	MF628,MF638, MDC525UP, MO825UP,MF622,MDC502HS
Option	ICON225
NOVATEL	MC950D
Zoom	4595
Vodafone	K3520-Z
Huawe	E270,E220
Sierra	AirCard 880U,875U,888
Quanta	GKXQCX

The list is continously updated at http://www.billion.com/compatible-3G.html

1. This router may require firmware modification for certain ADSL2/2+/Annex M DSLAMs.
2. Actual throughput and performance depends on the environment. Normally, the wireless speed is faster if you are closer to the router. The farther from the router you are, the more wireless range, and the speed will be slower.
3. The 3G / HSDPA data rate depends on your local service provider and your 3G / HSDPA modem.
4. By request of the Telco/ ISP projects
5. IPTV application may require subscribing to IPTV services from a Telco/ ISP

1.3 Hardware Specifications

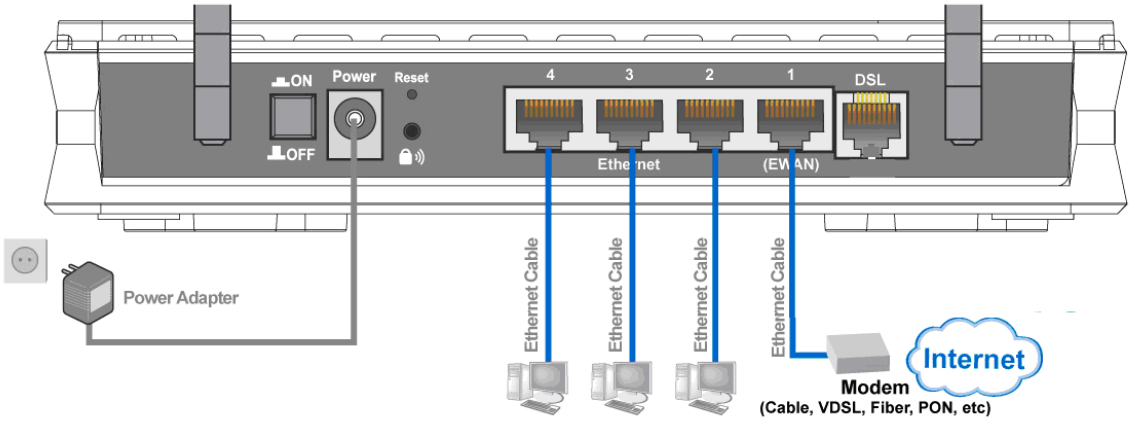
Physical Interface

- DSL: ADSL port
- Ethernet: 4-port 10/100M auto-crossover (MDI/MDI-X) switch
- EWAN: Ethernet port#1 can be configured to ADSL/Cable/VDSL/Fiber mode device (BiPAC 7300N *RE* only)
- USB 2.0 supports 3G/HSDPA modem backup (BiPAC 7300NX only)
- Factory default reset button
- WPS push button
- Power jack
- Power switch
- WLAN: 2 antennas

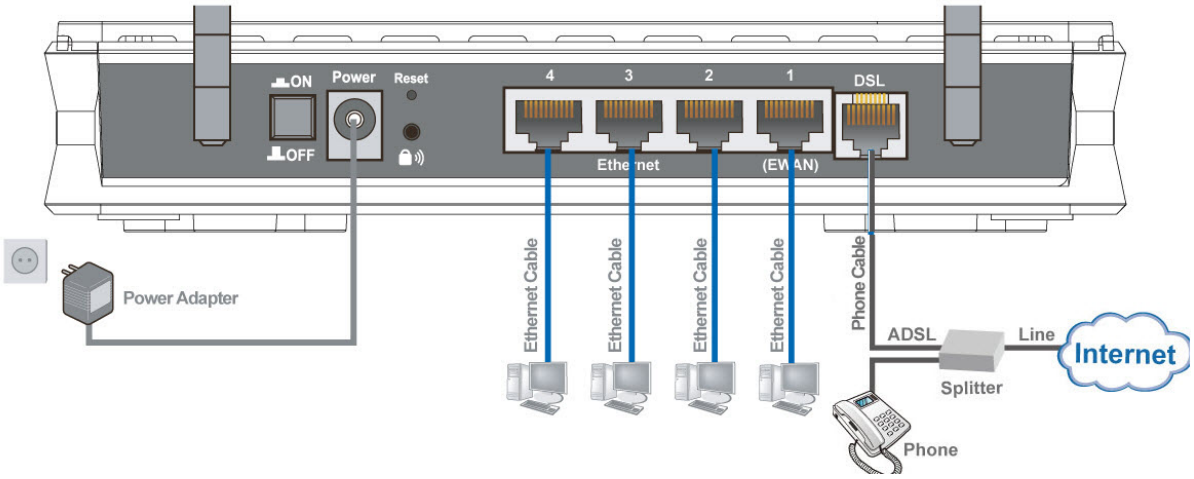
1.2 Applications of the devices

BiPAC 7300N *RE*

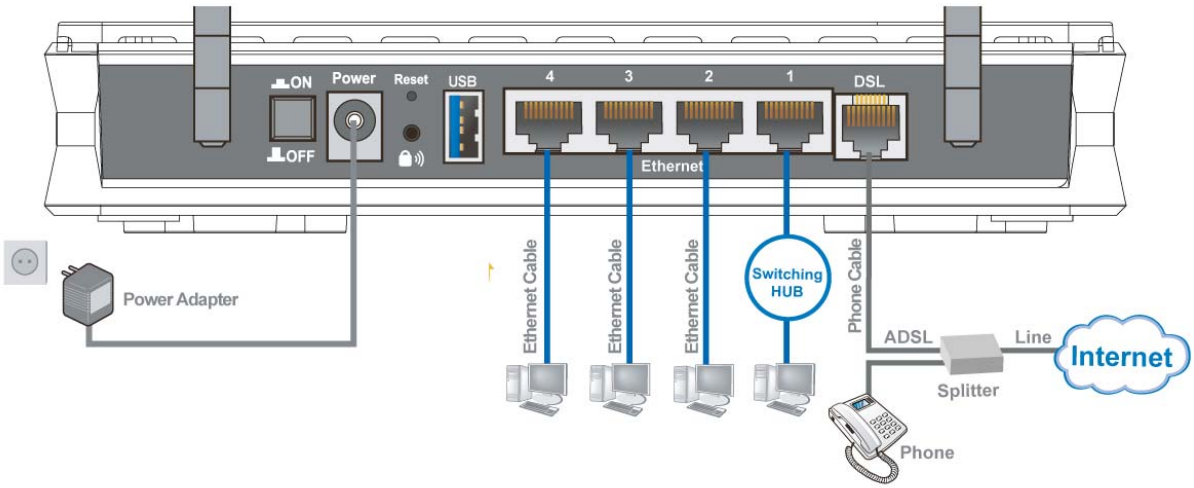
Broadband Router mode



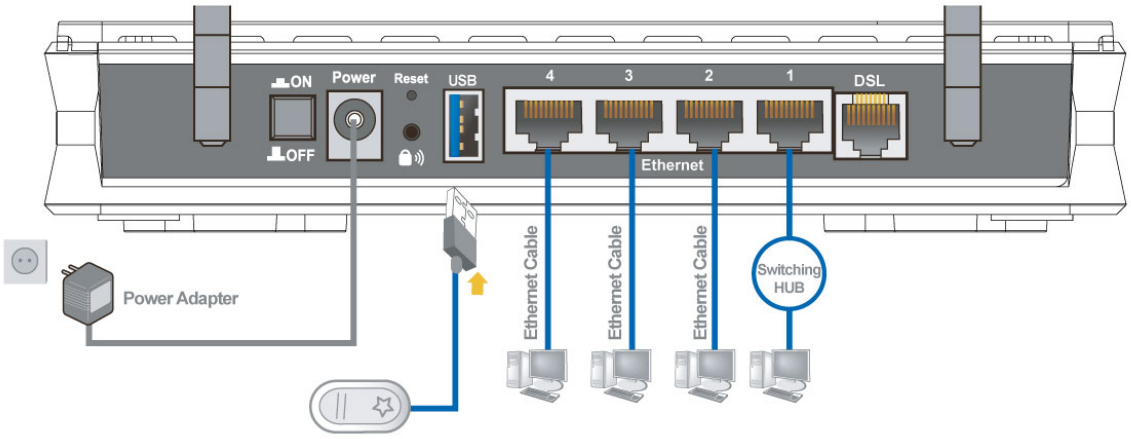
ADSL Router mode



BiPAC 7300NX



Broadband Router Mode



Chapter 2
Product Overview

2.1 Important Notes

Warning

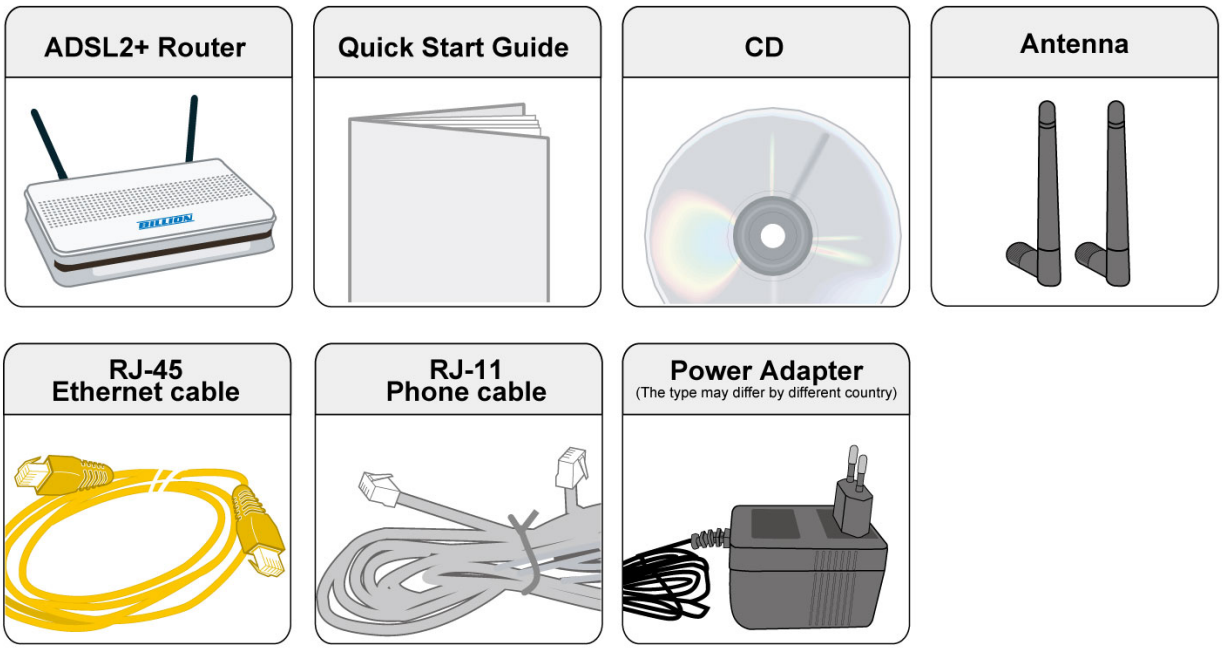
- ✓ Do not use the router in high humidity or high temperatures.
- ✓ Do not use the same power source for the router as other equipment.
- ✓ Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.

Attention

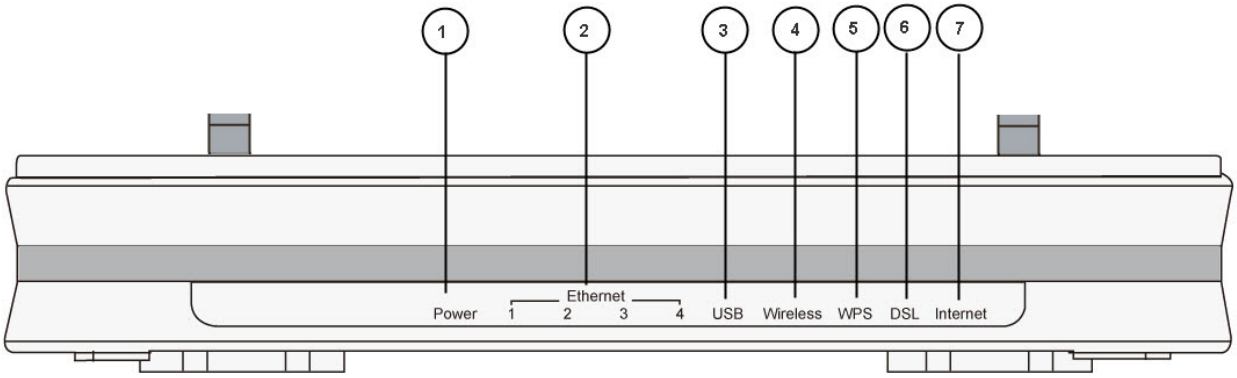
- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

2.2 Package Contents

- BiPAC 7300NX/N *RE* (3G) / Wireless-N ADSL2+ Firewall Router
- CD-ROM containing the on-line manual and QSG
- RJ-11 ADSL/telephone Cable
- Ethernet (RJ-45) Cable
- Power Adapter
- Quick Start Guide
- Two detachable antennas
- Splitter / Micro-filter (Optional)



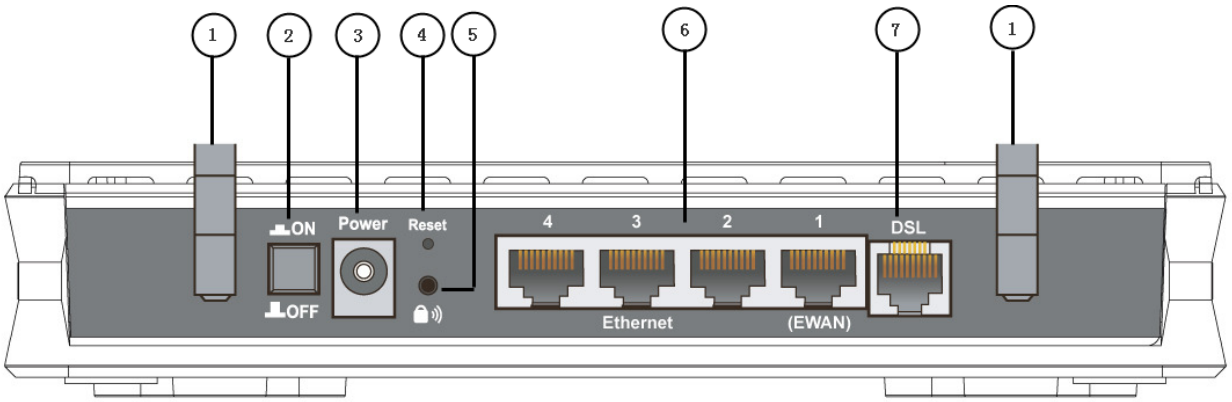
2.3 The Front LEDs



LED		Meaning
1	**Power**	Lit red while the flash is damage and cannot bring the system up. Lit green when the system is ready. Flashes green when the the system is rebooting or firmware upgrading.
2	**Ethernet Port 1 - 4**	Lit green when connected to an Ethernet device. Blinking when data is Transmitted / Received.
3	**USB(7300NX only)**	Lit when the router is connected to a USB device.
4	**Wireless**	Lit green when the wireless connection is established. Flashes when sending/receiving data.
5	**WPS**	Blinking when WPS is in progress.
6	**DSL**	Lit green when successfully connected to an ADSL DSLAM ("linesync").
7	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully.

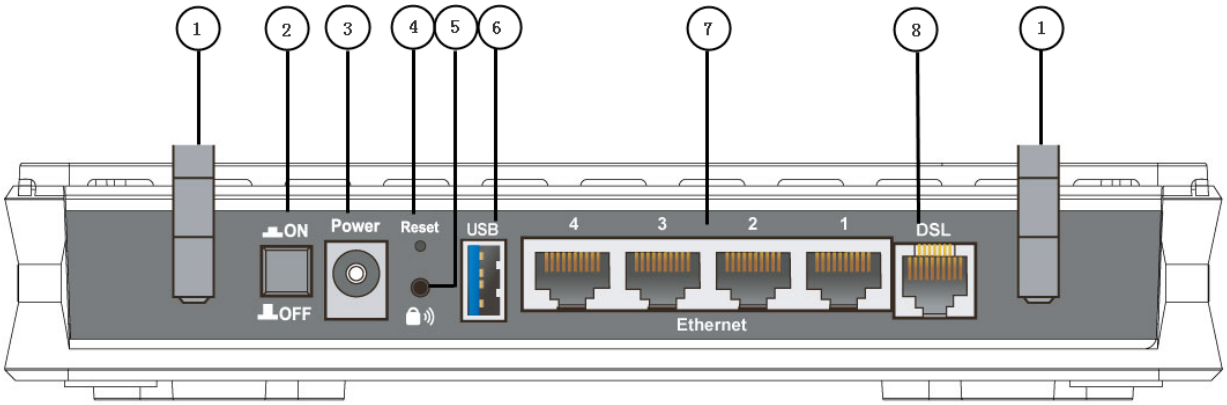
2.4 The Rear Ports

BiPAC 7300N *RE*



Port		Description
1	**Antenna**	Connect the antenna to this port.
2	**ON/OFF**	Power ON/OFF switch.
3	**Power**	Connect the supplied power adapter to this jack.
4	**Reset**	After the router is powered on, press this reset button using the end of paper clip or other small pointed object for 6 seconds and above to restore it to factory default settings. 1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash). 2. Recovery procedures for a lost web interface password.
5	**WPS**	Press the WPS button acoording to the following two to achieve different functions. (1)WPS: Press 2-6 seconds until WPS LED flashes green to trigger WPS function. (2) Wireless ON/OFF Switch: Press over 6 seconds after WPS LED is off to switch on wireless function. Press over 6 seconds again for disable wireless function.
6	**Ethernet**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps. ***Note: Only Ethernet port 1 can be used for EWAN.***
7	**DSL**	Connect the supplied RJ-11 (“telephone”) cable to this port when connecting to the ADSL/telephone network.

BiPAC 7300NX



Port		Description
1	**Antenna**	Connect the antenna to this port.
2	**ON/OFF**	Power ON/OFF switch.
3	**Power**	Connect the supplied power adapter to this jack.
4	**Reset**	After the router is powered on, press this reset button using the end of paper clip or other small pointed object for 6 seconds and above to restore it to factory default settings. 1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash). 2. Recovery procedures for a lost web interface password.
5	**WPS**	Press the WPS button acoording to the following two to achieve different functions. (1)WPS: Press 2-6 seconds until WPS LED flashes green to trigger WPS function. (2) Wireless ON/OFF Switch: Press over 6 seconds after WPS LED is off to switch on wireless function. Press over 6 seconds again for disable wireless function.
6	**USB**	Connect the USB cable to this port.
7	**Ethernet**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
8	**DSL**	Connect the supplied RJ-11 (“telephone”) cable to this port when connecting to the ADSL/telephone network.

The detail instruction in Reset Button

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):

Hold the *Reset Button* on the back of the modem in. Keep this button held in and turn on the modem. Once the lights on the modem have stopped flashing, release the *Reset Button.* The modem's emergency-reflash web interface will then be accessible via http://192.168.0.254 where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

Before powering on the router to enter the recovery process, please configure the IP address of the PC as 192.168.0.100 and proceed with the following step by step guide.

1. Power the router off.
2. Hold the "Reset Button".
3. Power on the router. Then Router's IP will reset to Emergency IP address (Say 192.168.0.254)
4. Download the firmware.

2.5 Cabling

One of the most common causes of problems is because of bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analog modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and to ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed being the wrong way around can cause problems with your ADSL connection, which includes frequent disconnections.

Chapter 3
Installation

You can configure the BiPAC 7300NX/N *RE* router through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux and Windows 7/Vista/98/NT/2000/XP/Me include a web browser as a standard application.

3.1 Before Configuration

PCs must have a properly installed Ethernet interface which connects to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range between 192.168.1.1 and 192.168.1.253). The easiest way is to configure the PC is to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface you are advised to **uninstall** any kind of software firewall on your PCs, as they can cause problems when trying to access the 192.168.1.254 IP address of the router.

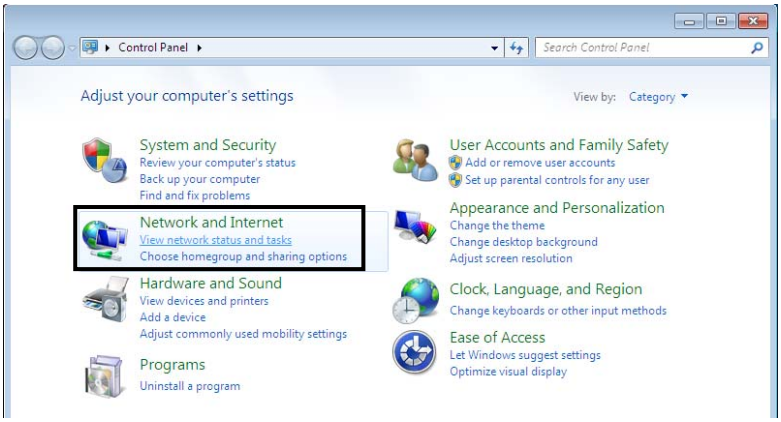
Please follow the steps below for installation on your PC's network environment. First of all, check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

Any TCP/IP capable workstation can be used to communicate with or through the BiPAC 7300NX/N *RE*. To configure other types of workstations, please consult the manufacturer's documentation.

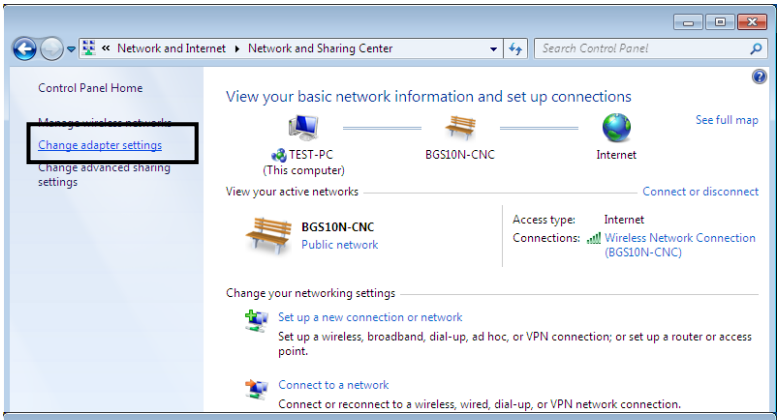
3.2 Network Configuration

3.2.1 Configuring a PC in Windows 7

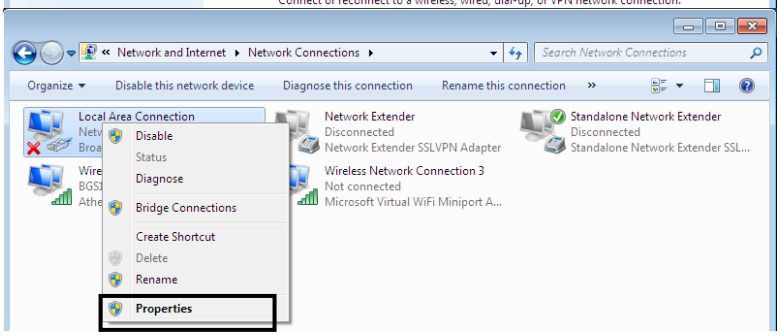
1. Go to **Start**. Click on **Control Panel**.
   Then click on **Network and Internet**.



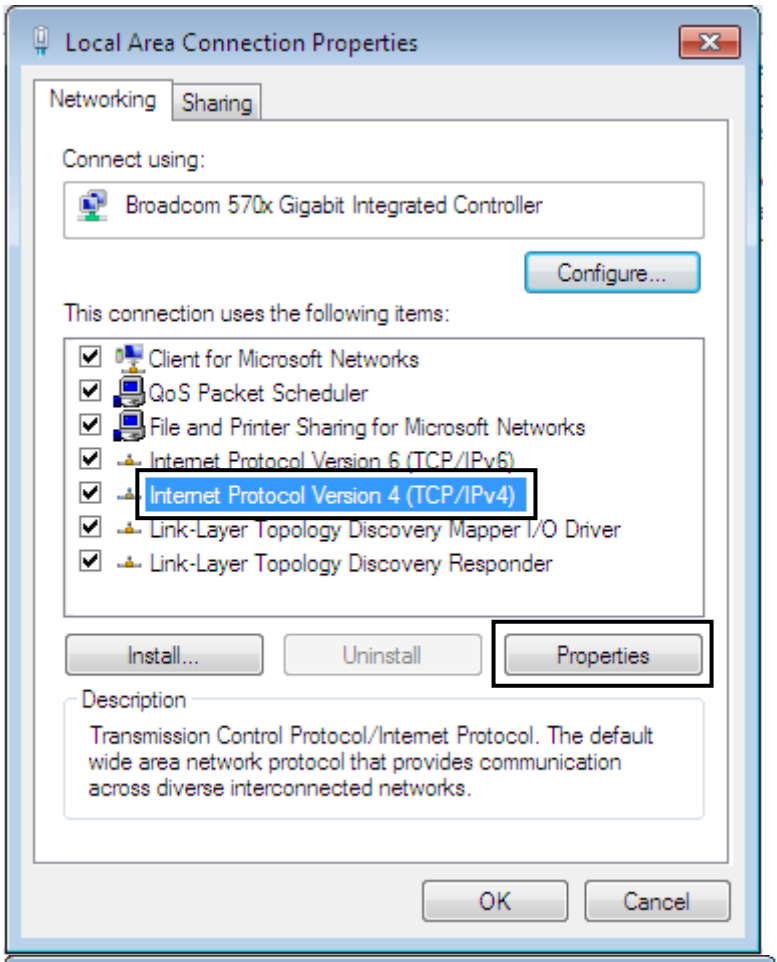
2. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.


Network and Internet
Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

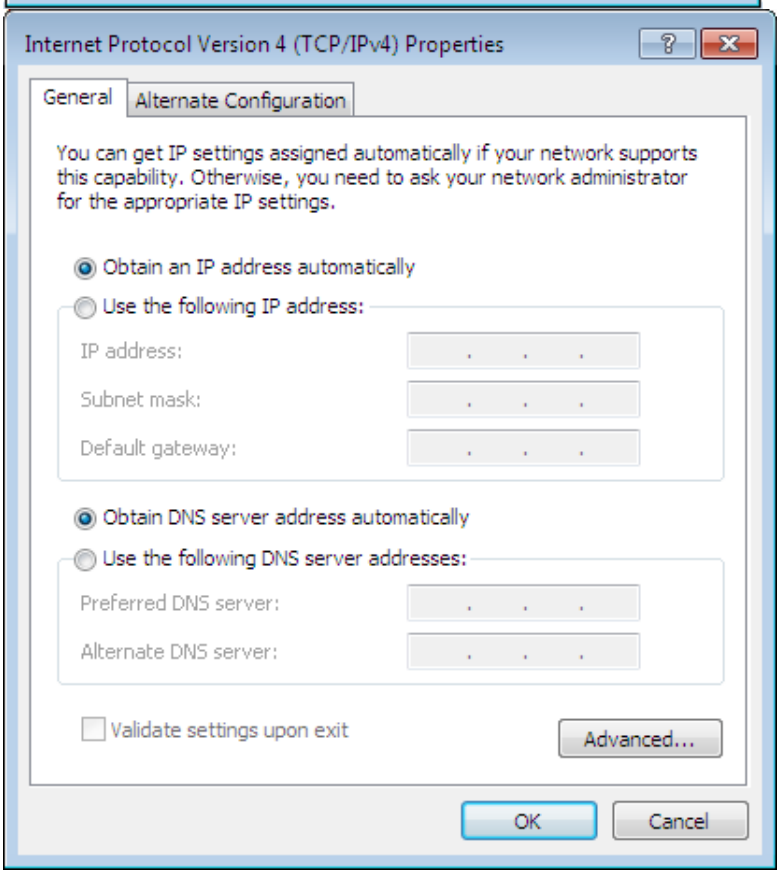


4. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

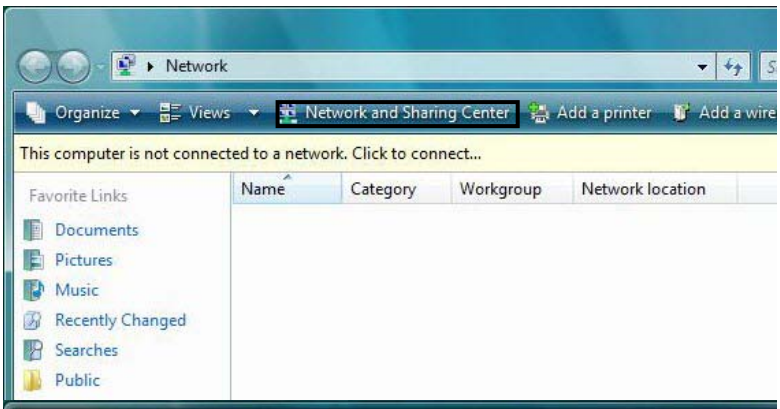
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

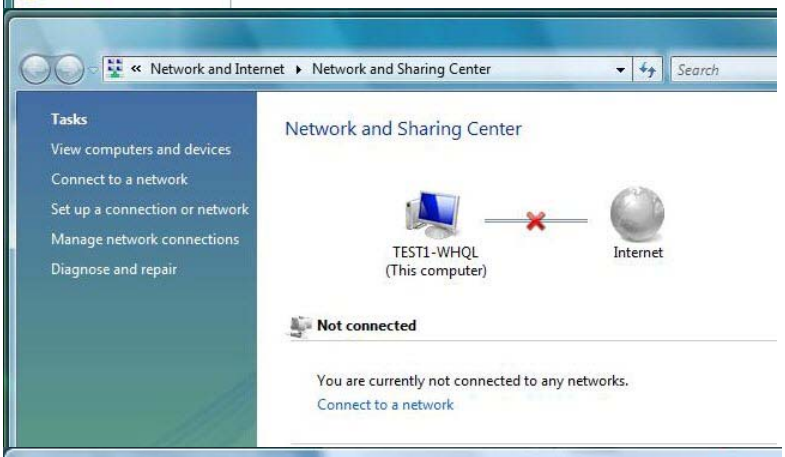
3.2.2 Configuring a PC in Windows Vista

1. Go to **Start**. Click on **Network**.

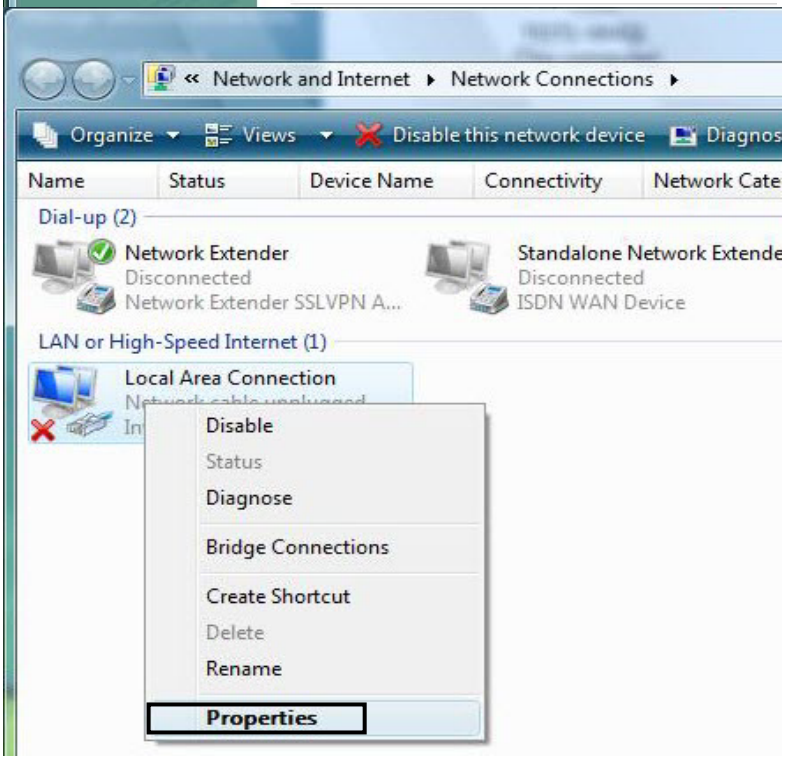
2. Then click on **Network and Sharing Center** at the top bar.



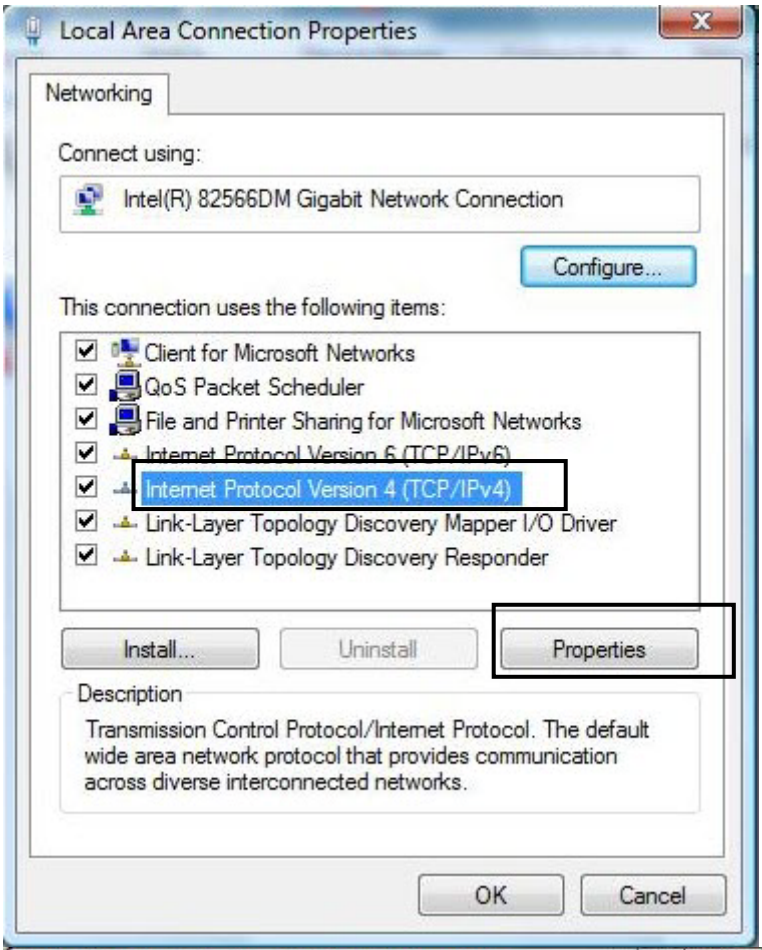
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

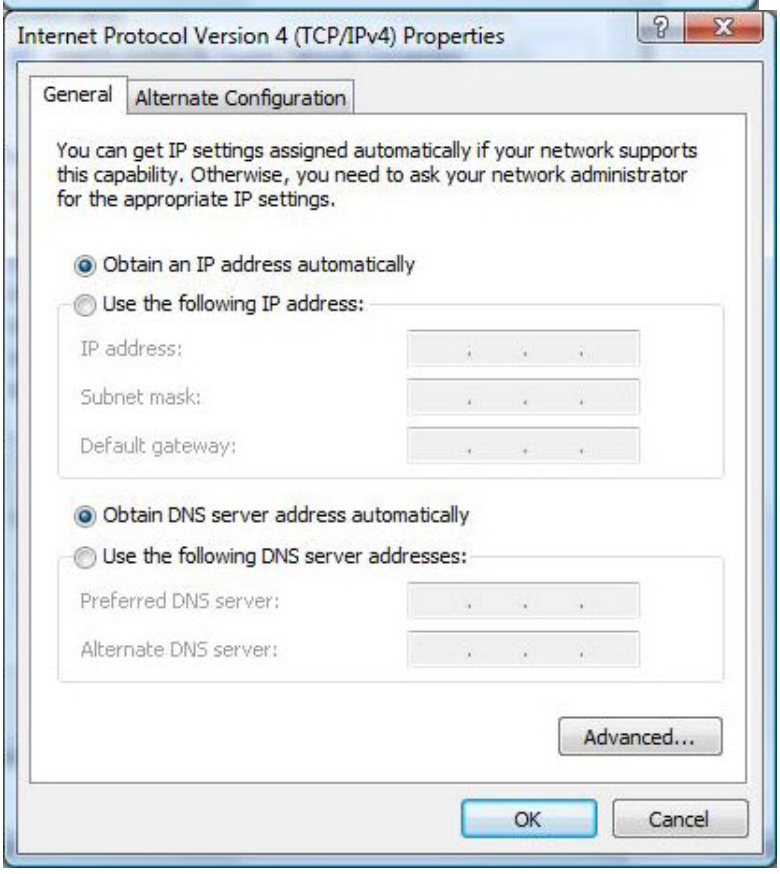


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



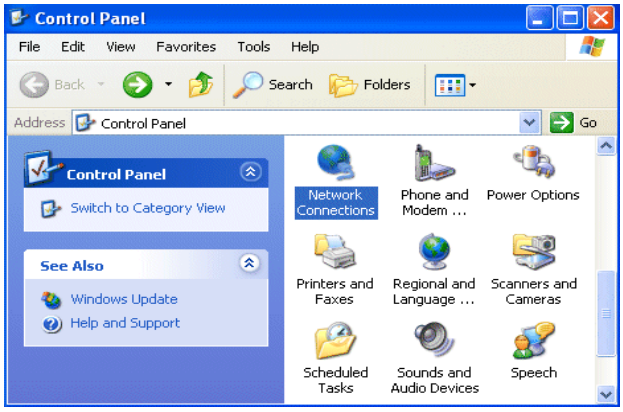
6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

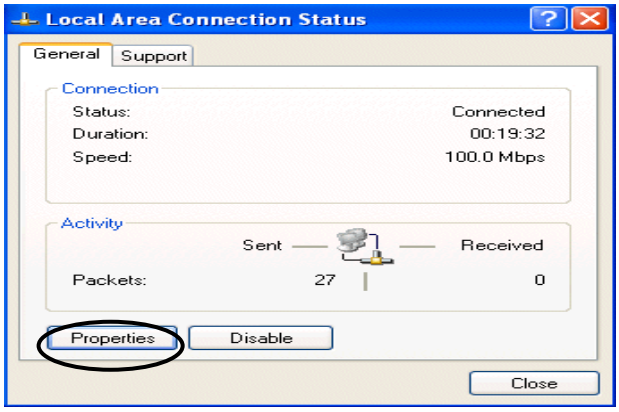

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

3.2.3 Configuring a PC in Windows XP

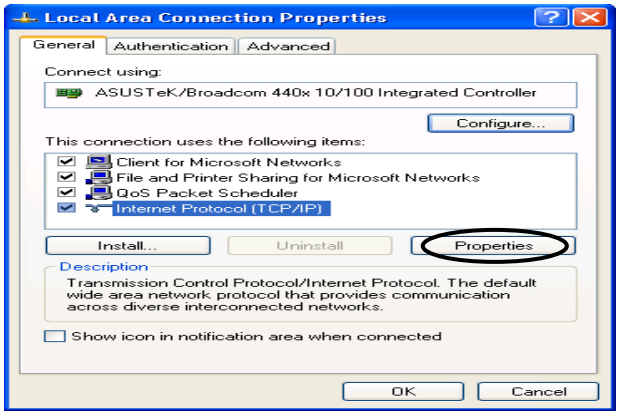
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

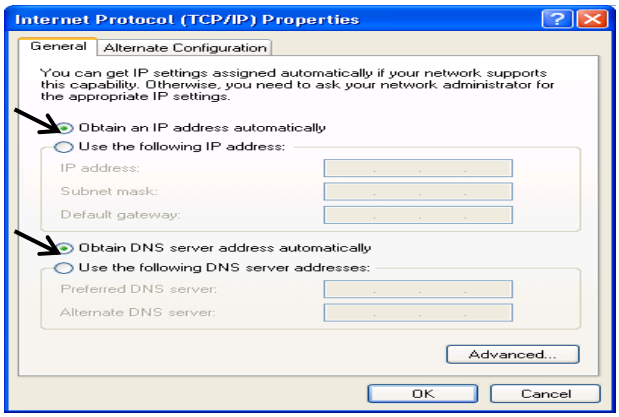


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.


Local Area Connection Properties
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

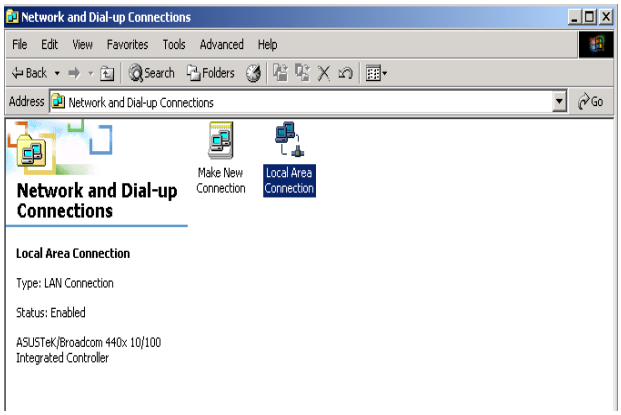
6. Click **OK** to finish the configuration.


Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

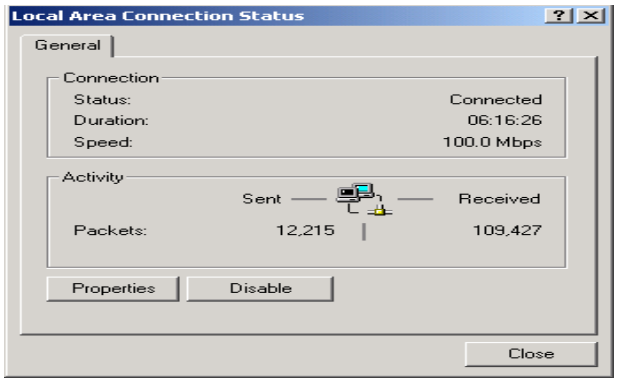
3.2.4 Configuring a PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

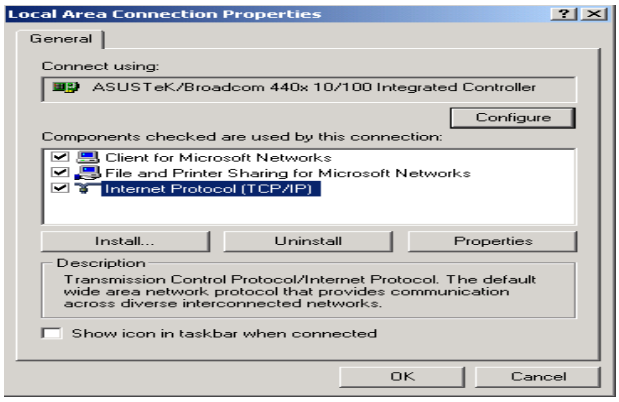
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window click **Properties**.

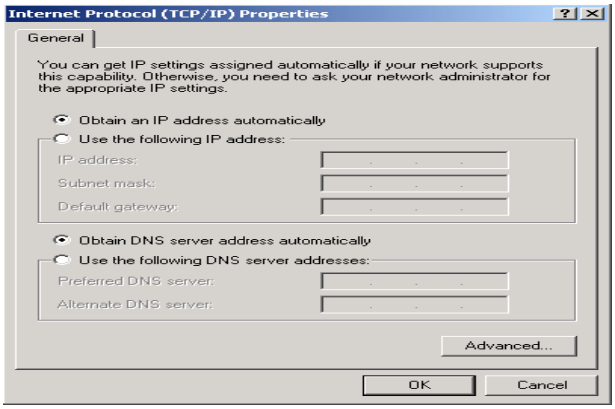


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



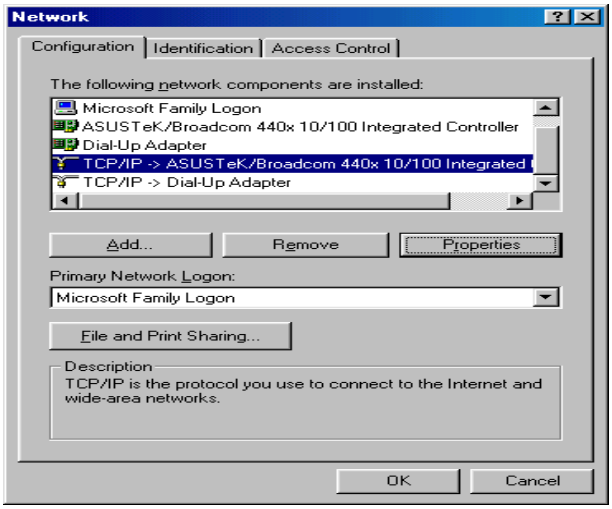
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

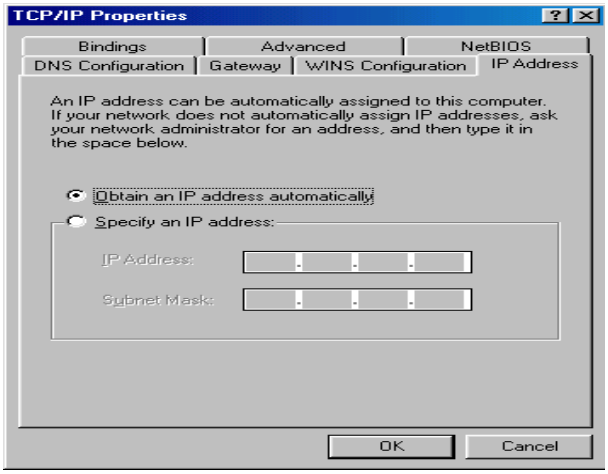
3.2.5 Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.



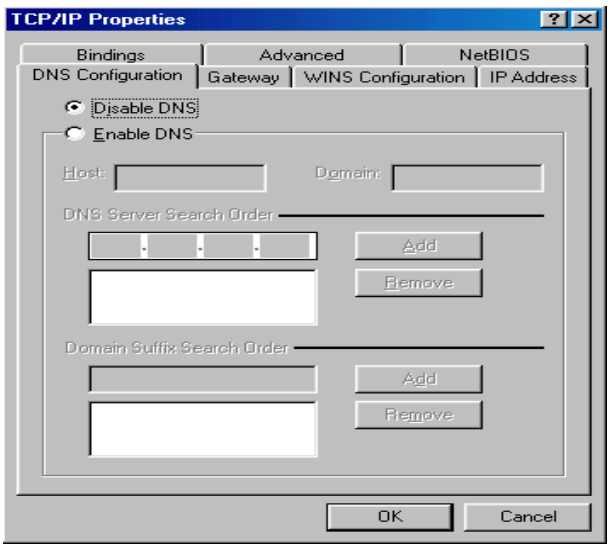
2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.

3. Select the **Obtain an IP address automatically** radio button.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

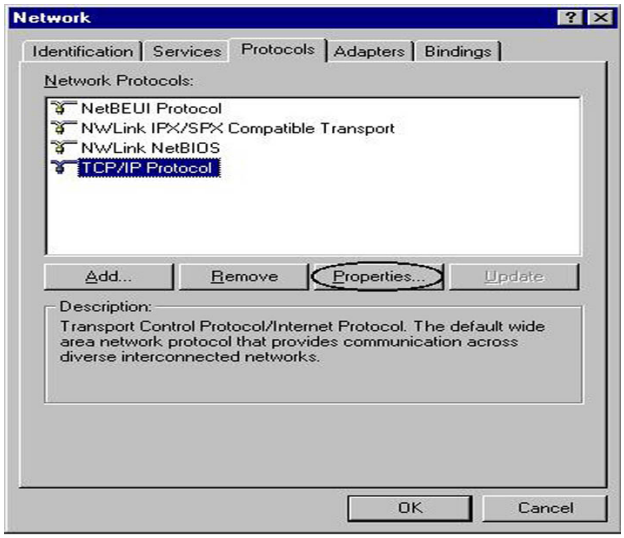
4. Then select the **DNS Configuration** tab.

5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



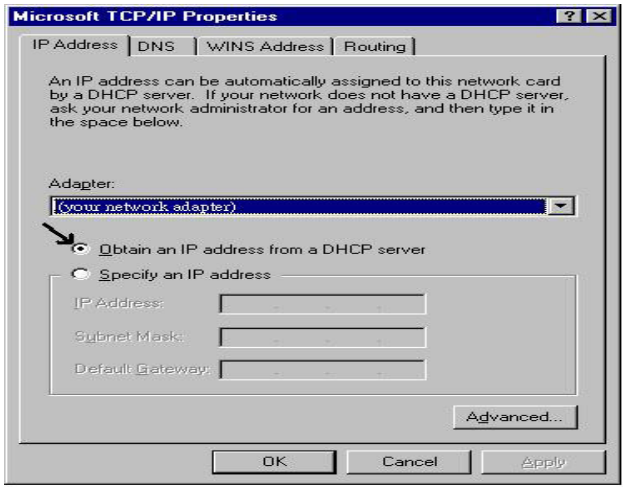
3.2.6 Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.



2. Select **TCP/IP Protocol** and click **Properties**.

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

3.3 Factory Default Settings

Before configuring the router, you need to know the following default settings.

- **Web Interface: (Username and Password)**
  - Username: admin
  - Password: admin

  The default username and password are "**admin**" and "**admin**" respectively.

Attention

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

- **LAN Device IP Settings:**
  - IP Address: 192.168.1.254
  - Subnet Mask: 255.255.255.0

- **ISP setting in WAN site:**
  - PPPoE

- **DHCP Server:**
  - DHCP server is enabled.
  - Start IP Address: 192.168.1.100
  - IP pool counts: 100

3.4 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are preset in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled in ports 1, 2, 3 and 4	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

3.5 Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) which kind of services are provided, such as PPPoE, PPPoA, MPoA or Pure Bridge.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

3.6 Configuring with your BiPAC 7300NX/N *RE*

1. To configure this device, you must have IE 5.0 / Netscape 4.5 or above installed
2. You may configure the router for Internet access in two ways:

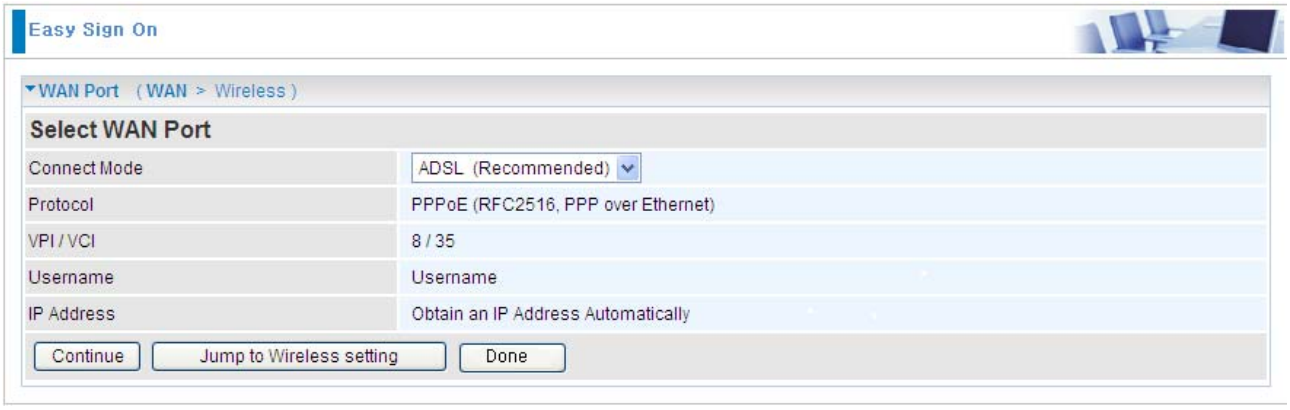
   (A) Easy Sign-On (EZSO) (B) Web Configuration

Easy Sign On

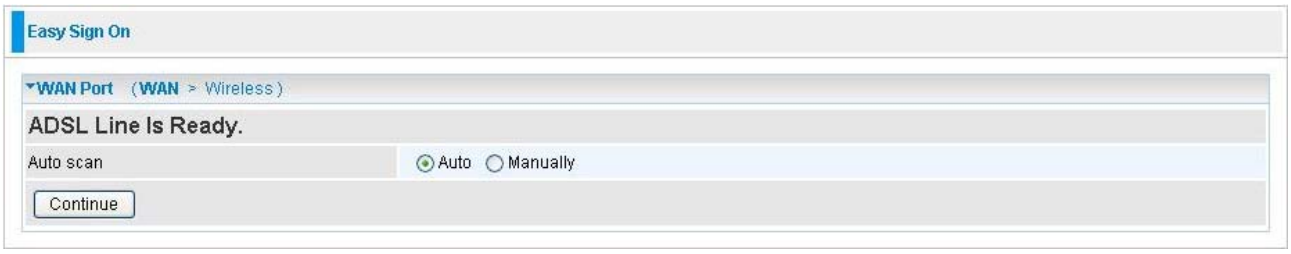
After setting up the router with appropriate cables plugged, proceed to load the internet browser to surf Internet, the EZSO WEB GUI will be popped up and request you to input some basic information you get from ISP. After this, you can surf Internet right away.

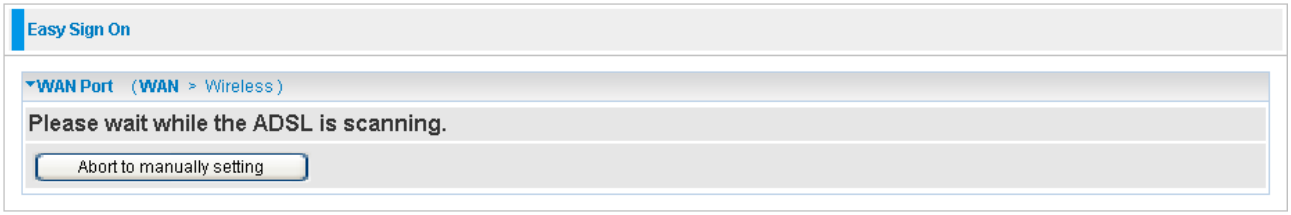
Follow the Easy Sign-On configuration wizard and it will guide you to complete the basic network configuration.

1. Click continue.

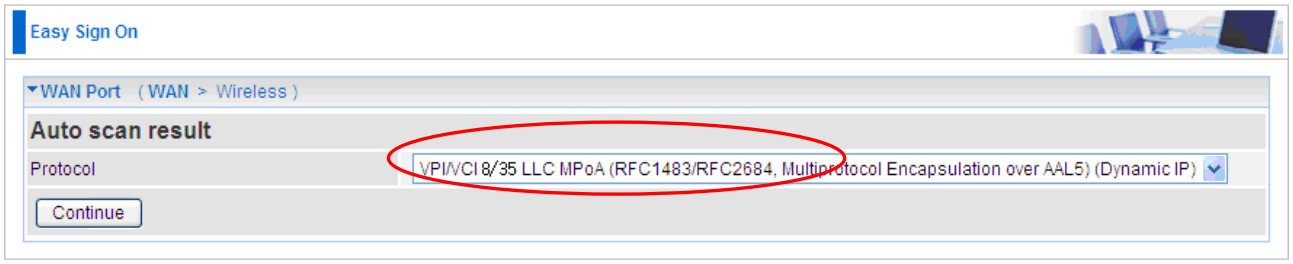


2. Choose “Auto” or “Manually” to scan ADSL information.

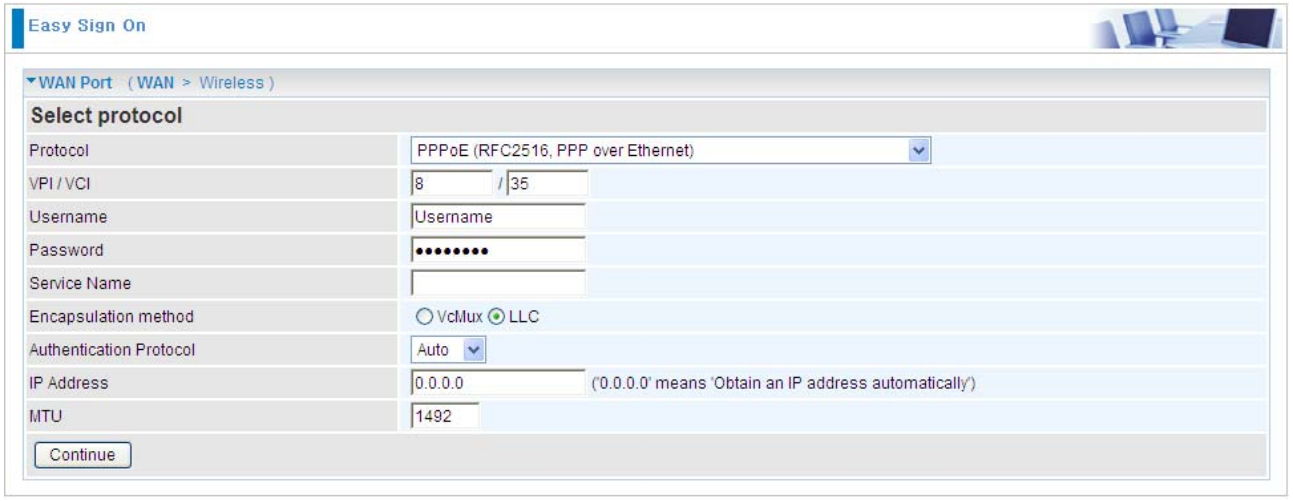




3. Show Auto scan result - Protocol information.

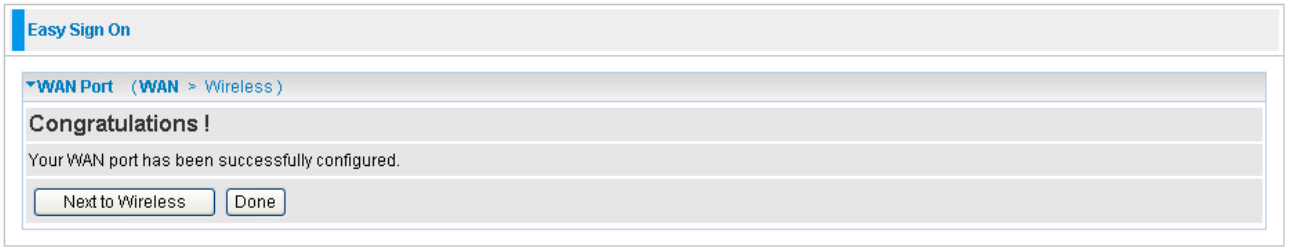

Easy Sign On
WAN Port (WAN > Wireless)
Auto scan result
Protocol
VPI/VCI 8/35 LLC MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5) (Dynamic IP)
Continue

4. Please enter **"Username"** and **"Password"** as supplied by your ISP (Internet Service Provider) and click continue.

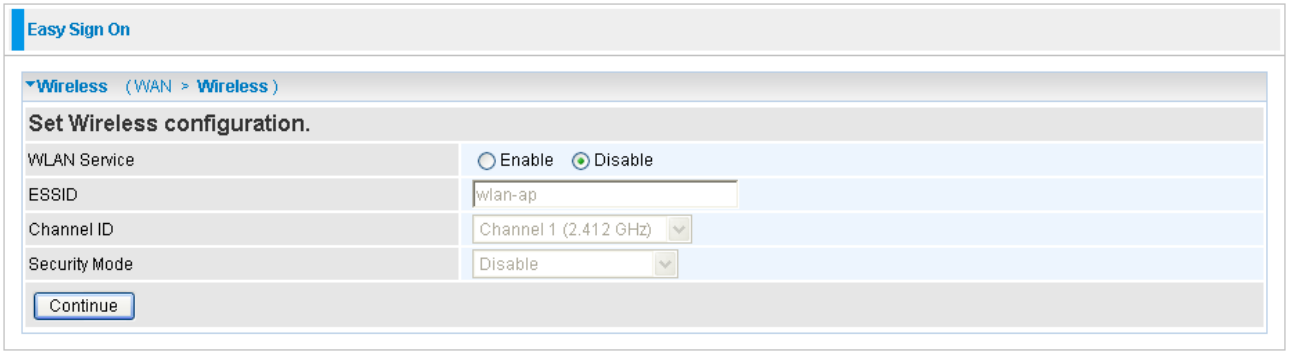


5. Wait for the device to be configured.

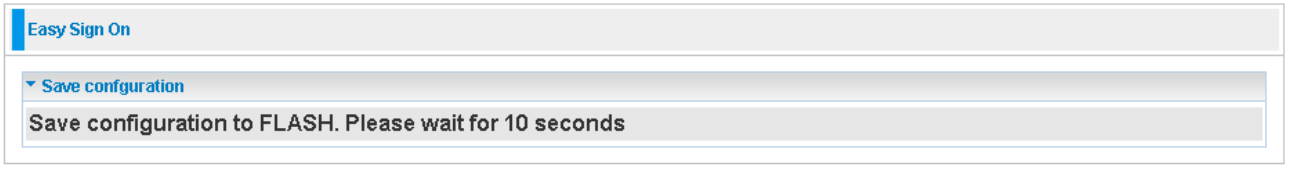
6. You've have completed the WAN port setup and now click "Next to Wireless" to proceed to the wireless configuration.



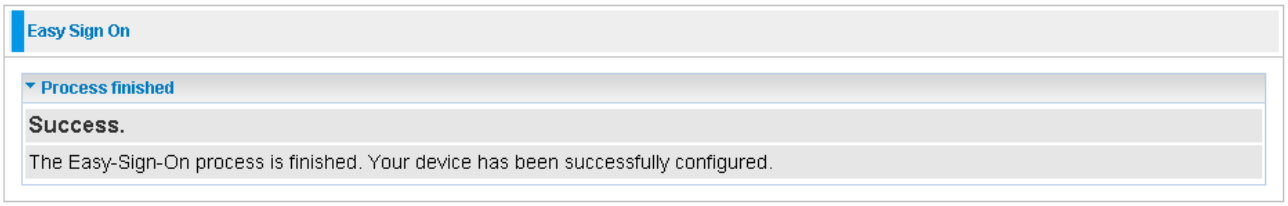
7. Please configure the Wireless LAN setting and click Continue.



8. Save Configuration.

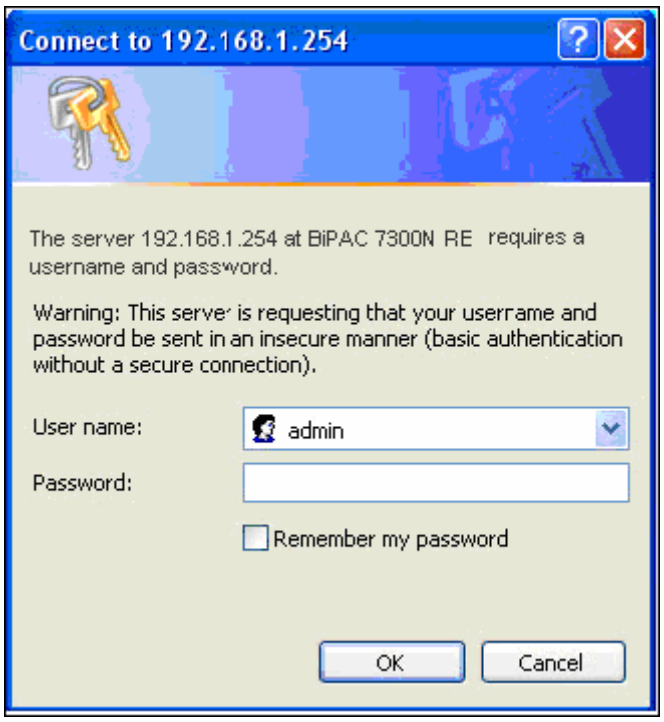


9. Congratulations!! You've completed the setup procedure and you are now ready to surf the Internet, enjoy.

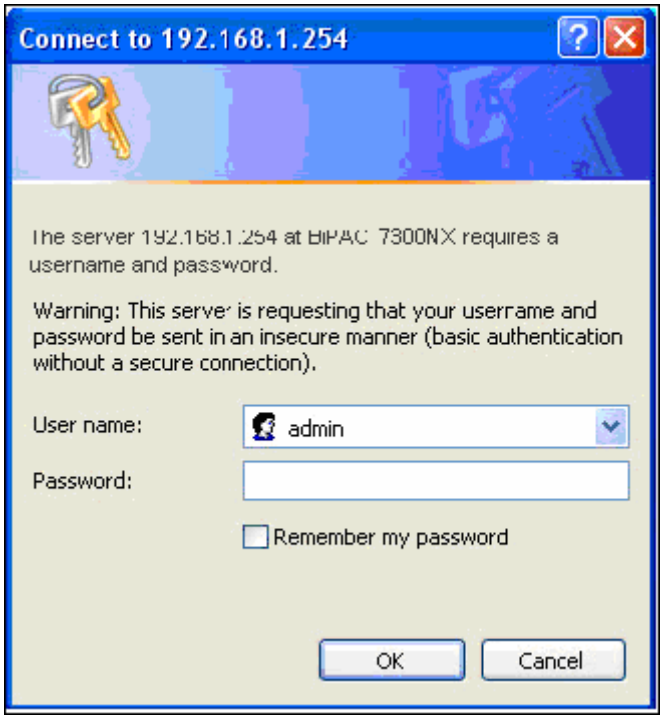

Easy Sign On
Process finished
Success.
The Easy-Sign-On process is finished. Your device has been successfully configured.

Web Configuration

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click "**Go**", a user name and password prompt window appears. The default username and password are **"admin"** and **"admin"** respectively.


Connect to 192.168.1.254
The server 192.168.1.254 at BiPAC 7300N RE requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Congratulations! You have successfully logged in to your BiPAC 7300N *RE* Router!


Connect to 192.168.1.254
The server 192.168.1.254 at BiPAC 7300NX requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

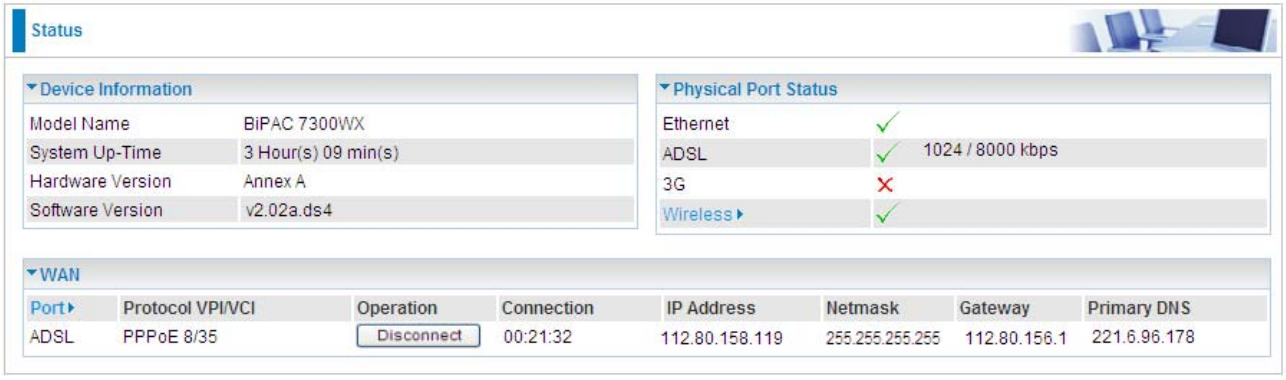
Congratulations! You have successfully logged in to your BiPAC 7300NX Router!

Chapter 4
Basic Configuration

Once you have logged on to your BiPAC 7300NX/N *RE* Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Advanced** (Switch to Advanced Configuration mode)
- **Status**
- **Quick Start**
- **WAN**
- **WLAN**

4.1 Status



(BiPAC 7300NX for example)

Device Information

- **Model Name:** Provide a name for the router for identification purposes.
- **System Up-Time:** Records system up-time.
- **Hardware Version:** Device version
- **Software Version:** Firmware version

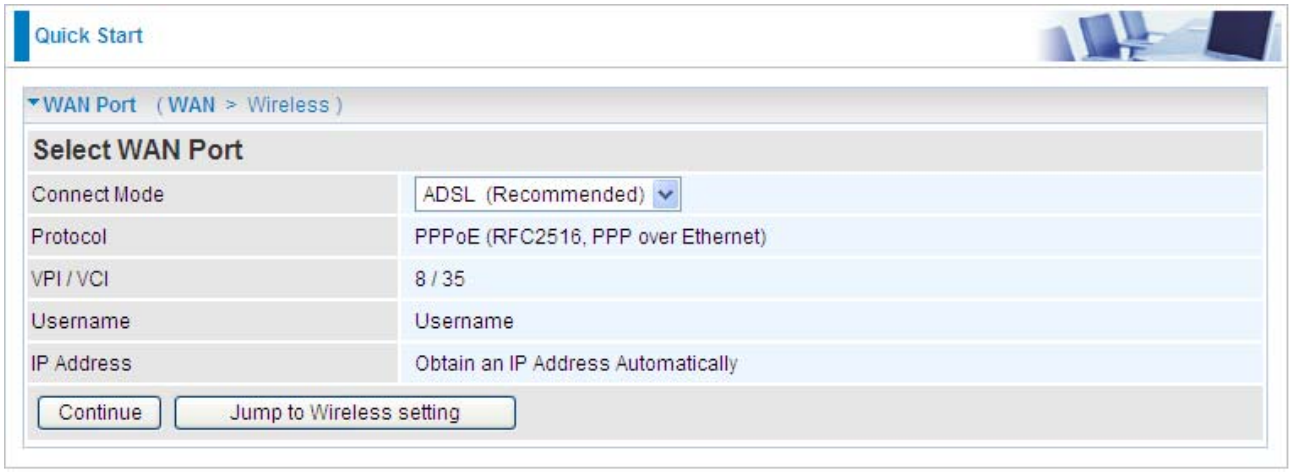
Physical Port Status

- **Port Status:** Users can look up to see if they are connected to Ethernet, ADSL, 3G (7300NX only), EWAN (7300N *RE* only) or Wireless.

WAN

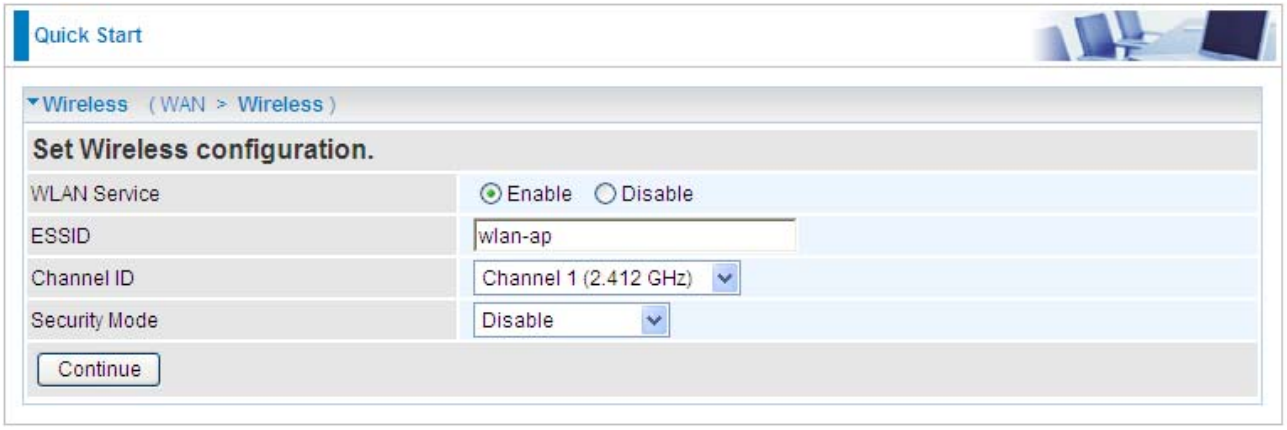
- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** Current available operation.
- **Connection:** The current connection status.
- **IP Address:** WAN port IP address.
- **Net mask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.
- **Primary DNS:** The IP address of the primary DNS server.

4.2 Quick Start



For the exactly steps, turn to **Advanced –Quick Start** for help.

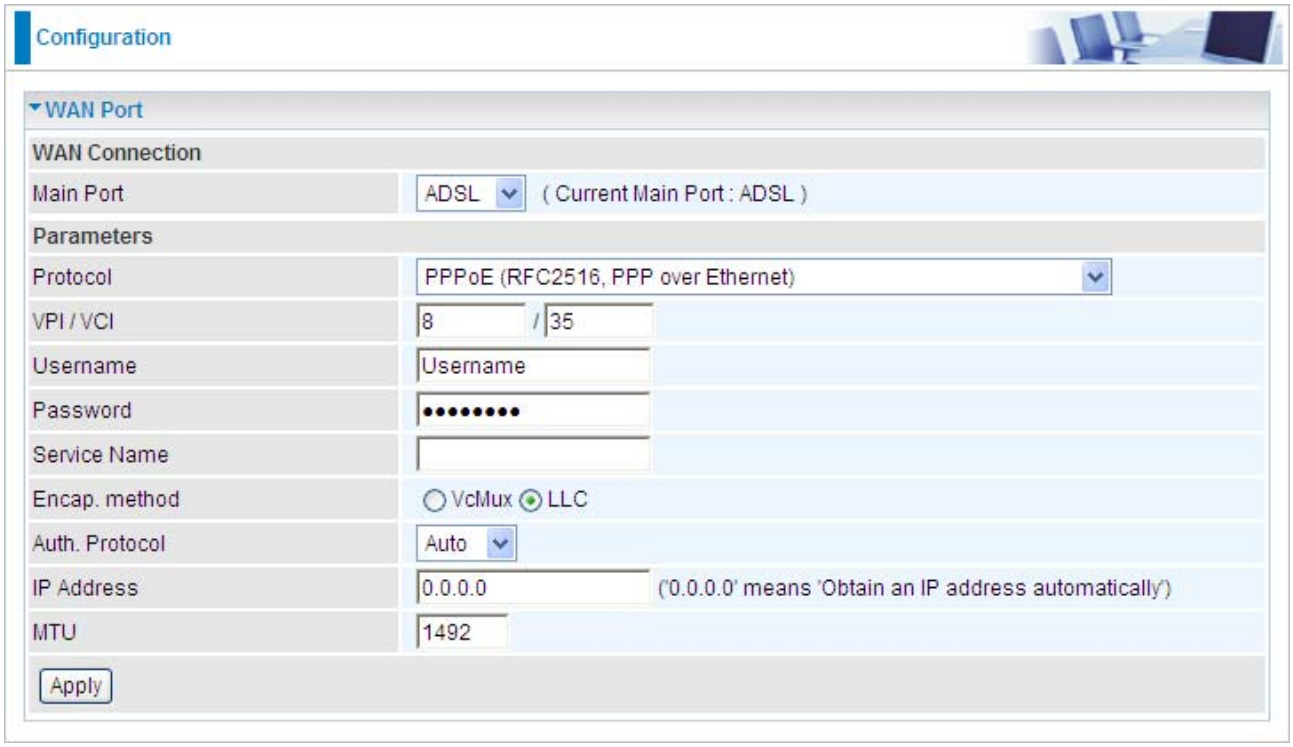
Set Wireless configuration



- **WLAN Service:** Default setting is set to **Enable**.
- **ESSID:** The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.
- **Channel ID:** Select the ID channel that you would like to use.
- **Security Mode:** You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**. For more information , turn to wireless security for help.

4.3 WAN

ADSL



- **Main Port:** Select the connection mode from the drop-down menu, here ADSL.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)
- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Auth. Protocol:** Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

For detail, please turn to **ADSL profile.**

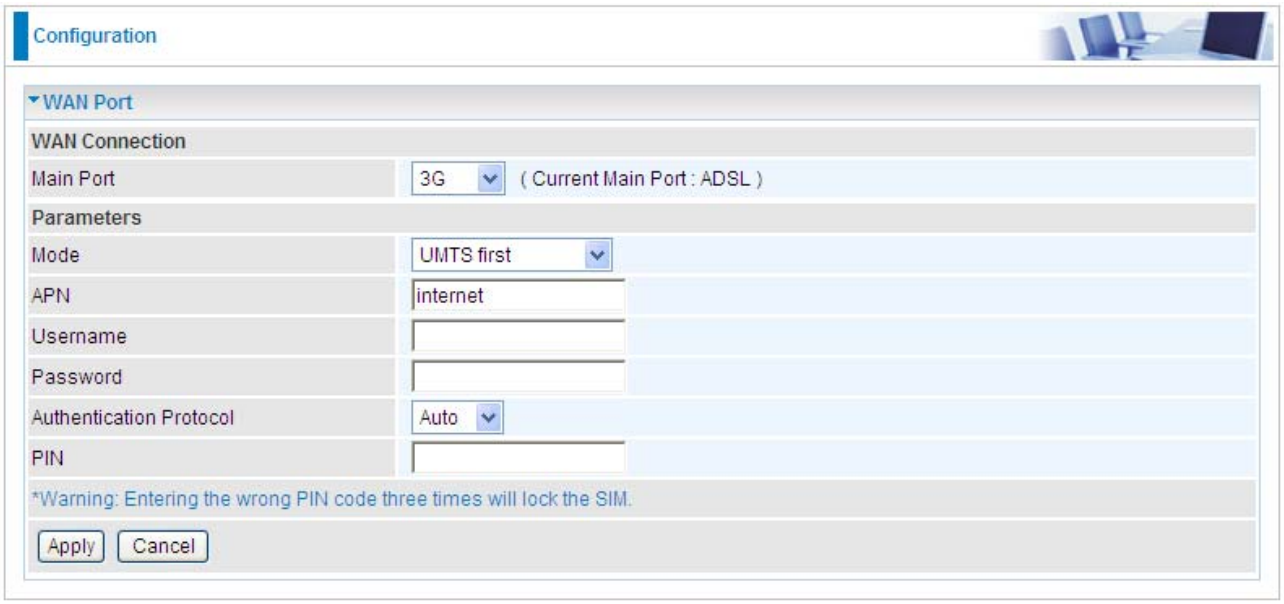
EWAN (BiPAC 7300N *RE* only)

Main Port: Select the connection mode from the drop-down menu, here EWAN.

Protocol: select the protocol used: Obtain an IP Address Automtically, Fixd IP Address or PPPoE.

For detail, please turn to **EWAN Profile .**

3G (BiPAC 7300NX only)



Mode: There are 5 options of phone service standards: GSM only, UTMS only, GPRS/EDGE first, UMTS first, and Automatic. If you are uncertain what services are available to you, and then please select Automatic.

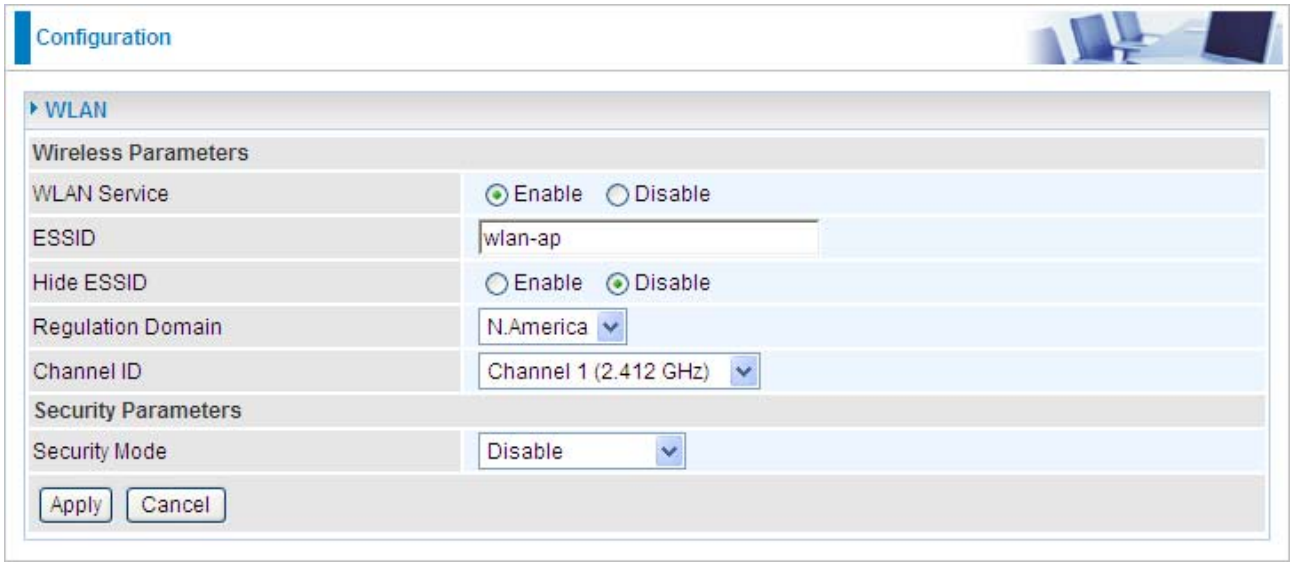
APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. Some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your ISP.

Authentication Protocol: Default is Auto. Please consult your ISP on whether to use PAP, CHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

4.4 WLAN



WLAN Service: Default setting is set to **Enable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable.**

⊙ **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hided in stead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.

⊙ **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

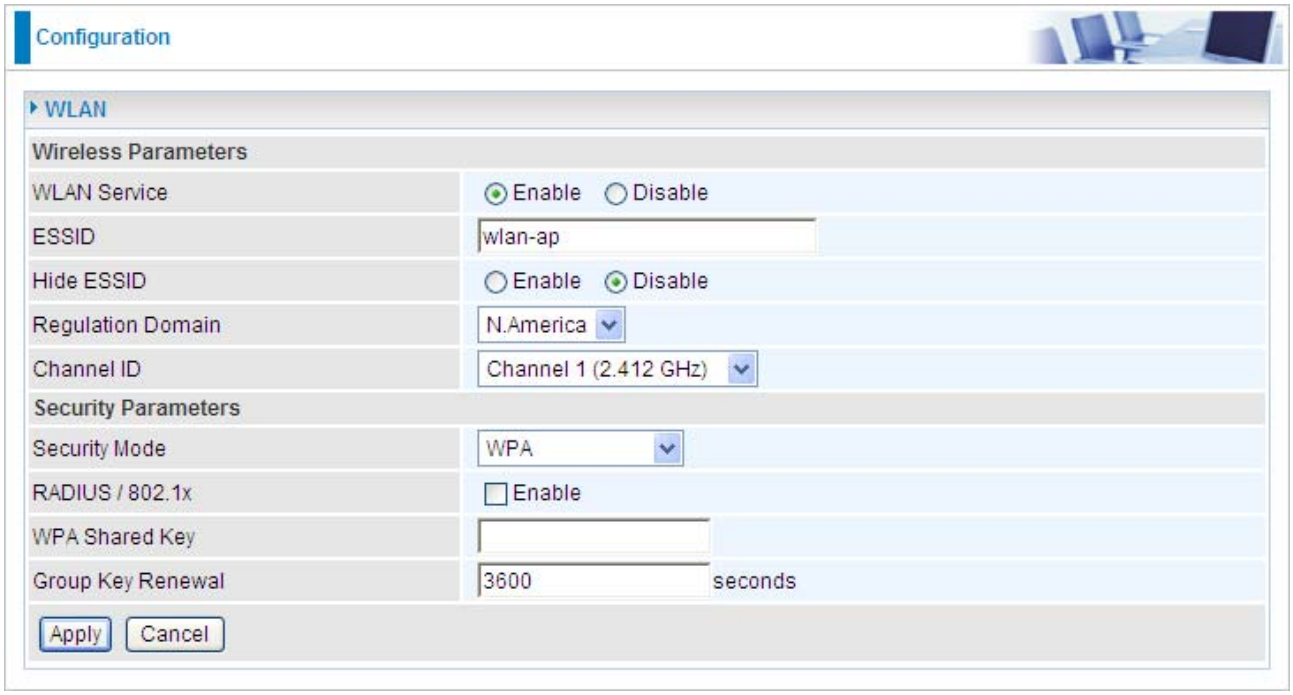
Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

Security Parameters

WPA or WPA2

WPA and WPA2 pre-shared keys are an authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.



WLAN Service: Default setting is set to Enable. If you want to use wireless, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable.**

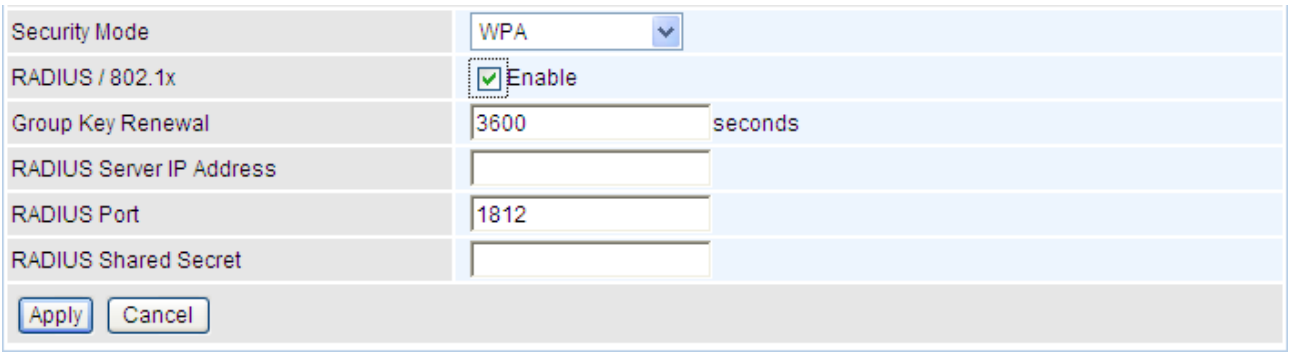
⊙ **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hided in stead of broadcasting, thus when wireless client searches for

this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.

⊙ **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

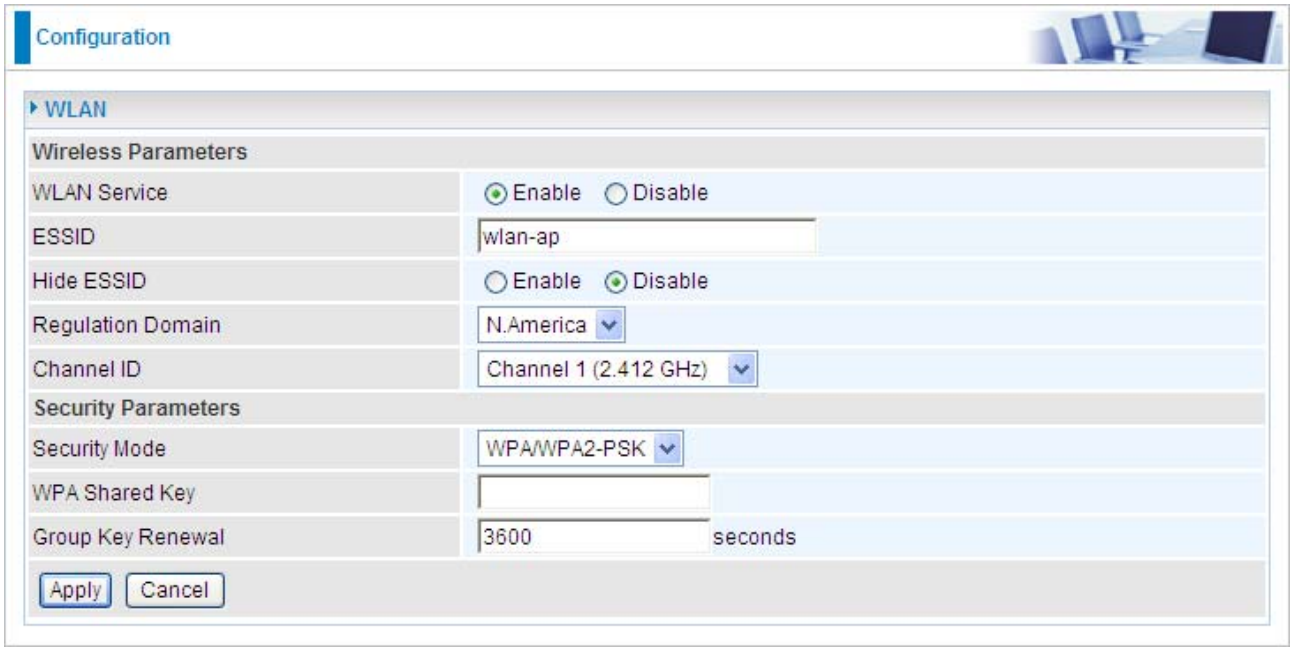
- **Channel ID:** Select the channel ID that you would like to use.
- **Security Mode:** You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.
- **RADIUS/802.1x:** You can enable or disable the RADIUS(Remote Authentication Dial In User Service) service.
- **WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Group Key Renewal:** The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

If you want to enable the RADIUS function, check Enable and then do the following settings.



- **RADIUS Server IP Address:** The IP address of RADIUS authentication server.
- **RADIUS Server Port:** The port number of RADIUS authentication server here. Default value is 1812.
- **RADIUS Shared Secret:** The password of RADIUS authentication server.

WPA / WPA2 Pre-Shared Key



WLAN Service: Default setting is set to Enable. If you want to use wireless, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the channel ID that you would like to use.

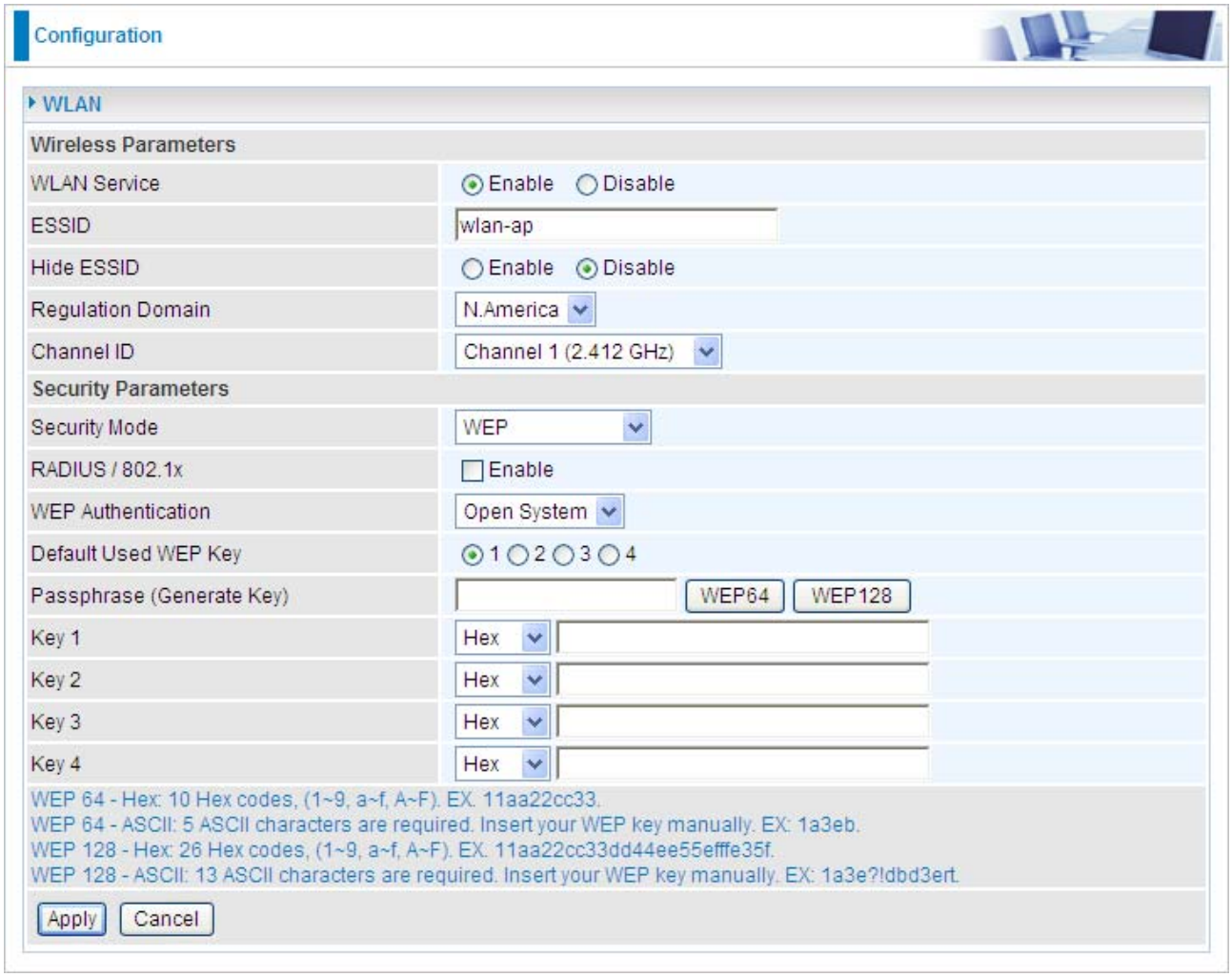
Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and the key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

Note: Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).

WEP



WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

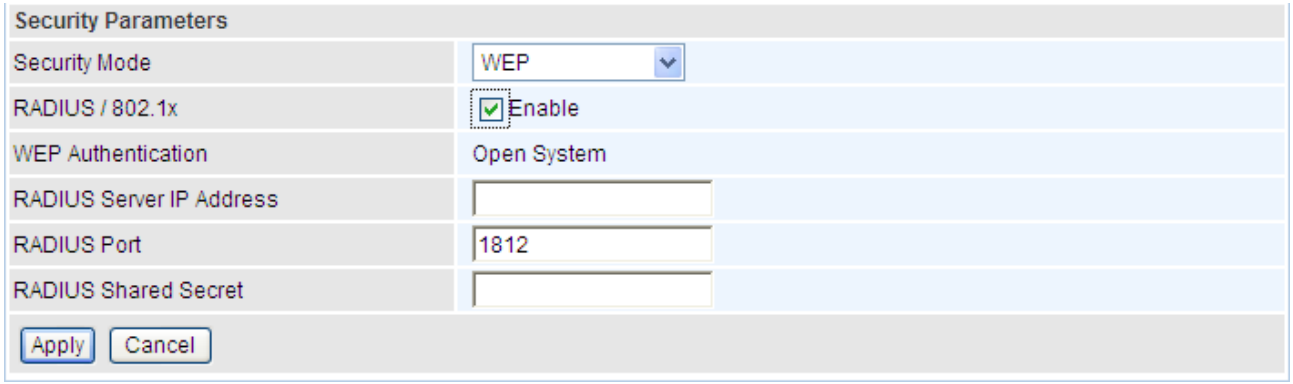
Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.
Note: Wireless performance may degrade if the selected channel ID is already being occupied

Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.
RADIUS / 802.1x: You can disable or enable the RADIUS service.
WEP Authentication: To prevent an unauthorized wireless station from accessing the data transmitted over the network, the router offers a secure data encryption, known as WEP. There are 3 options to select from: **Open System, Shared key** or **both**.
Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.
Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.
Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be either HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS function, check **Enable** and then do the following settings.



RADIUS Server IP Address: The IP address of RADIUS authentication server.
RADIUS Server Port: The port number of RADIUS authentication server here. Default value is 1812.
RADIUS Shared Secret: The password of RADIUS authentication server.
Click Apply to confirm the settings.

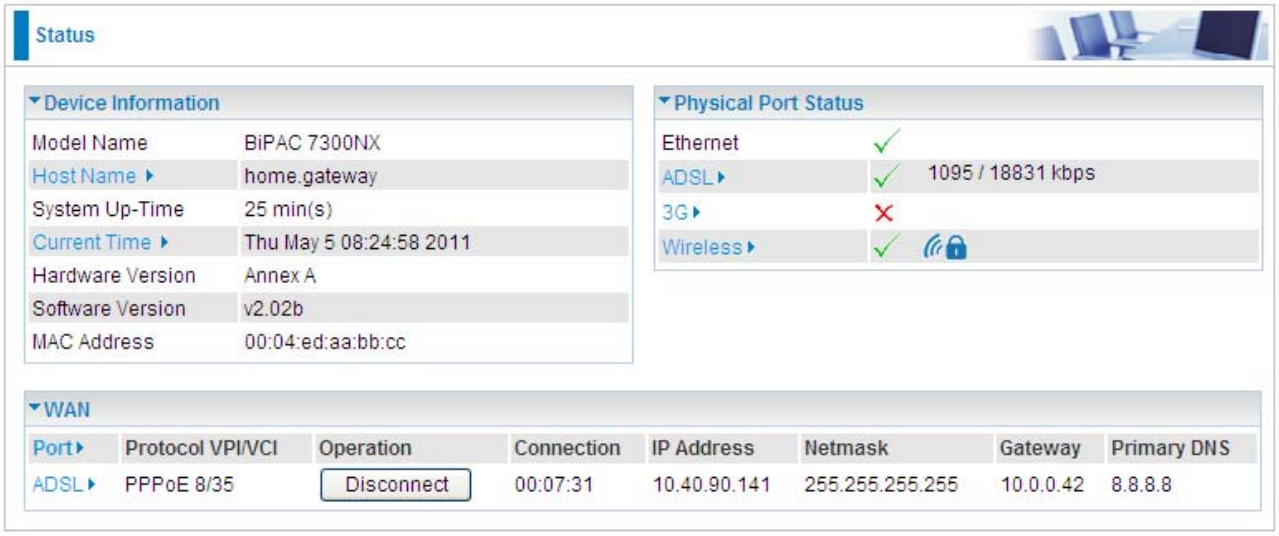
Chapter 5
Advanced Configuration

Once you have logged on to your BiPAC 7300NX/N *RE* Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Basic** (Switch to Basic Configuration Mode)
- **Status** (ADSL Status, 3G Status (BiPAC 7300NX only), ARP Table, DHCP Table, System Log, Firewall Log, UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, USB (BiPAC 7300NX only) Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced)

The following sections provide an overview of the settings available for configuring your router.

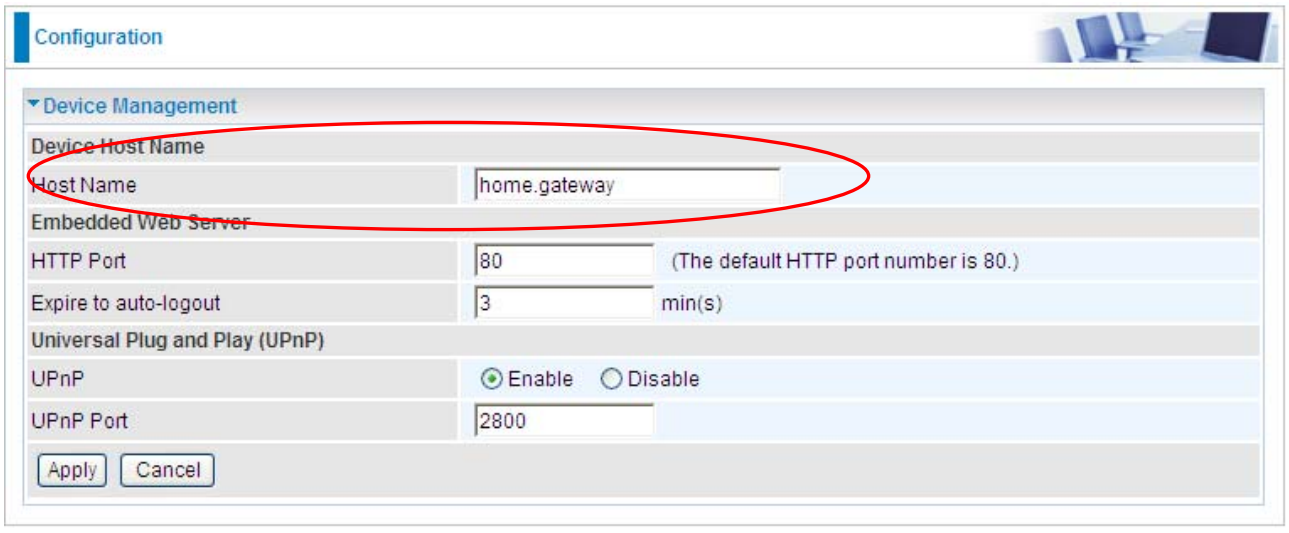
5.1 Status



(BiPAC 7300NX for example)

Device Information

- **Host Name:** Provide a name for the router for identification purposes. Host Name lets you change the router name.



- **System Up-Time:** Records system up-time.
- **Current time:** Set the current time. See the Time Zone section for more information.
- **Hardware Version:** Device version.
- **Software Version:** Firmware version.
- **MAC Address:** The LAN MAC address.

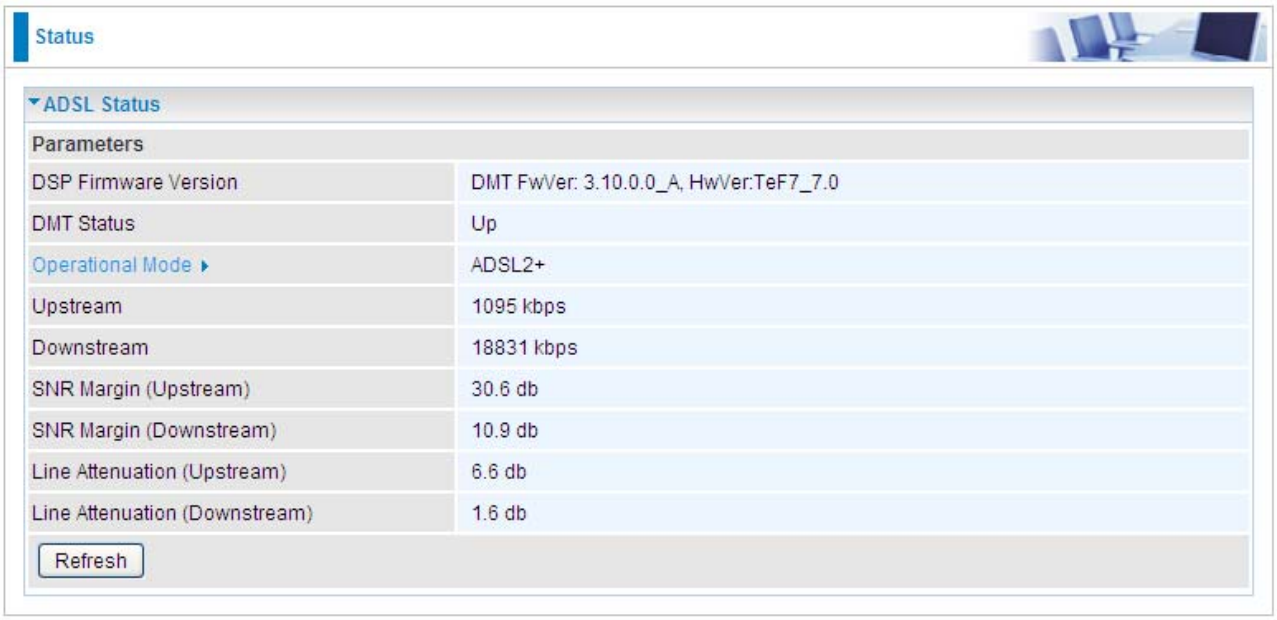
WAN

- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** Current available operation.
- **Connection:** The current connection status.
- **IP Address:** WAN port IP address.
- **Net mask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.
- **Primary DNS**: The IP address of the primary DNS server.

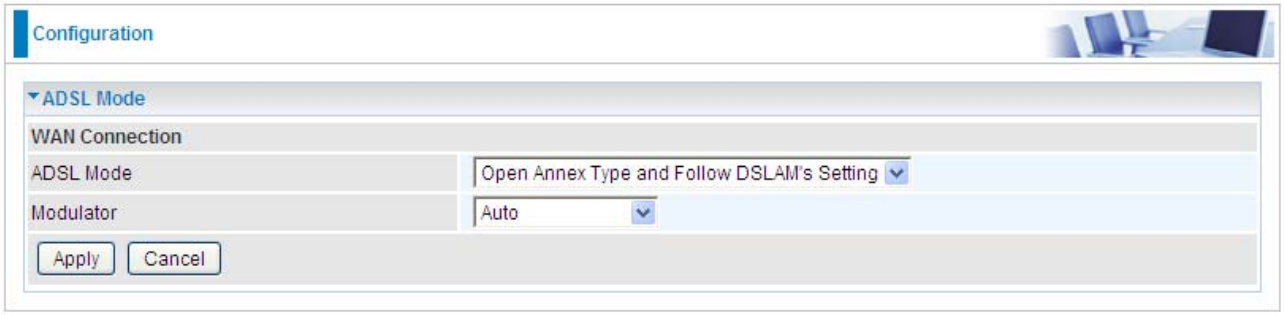
Physical Port Status

- **Port Status:** User can look up to see if they are connected to Ethernet, ADSL, 3G (7300NX only), EWAN (7300N *RE* only) or Wireless.

5.1.1 ADSL Status



- **DSP Firmware Version:** DSP code version
- **DMT Status:** Current DMT Status
- **Operational Mode:** To show the state when user select “AUTO” on connect mode. Click the link, the following will appear.

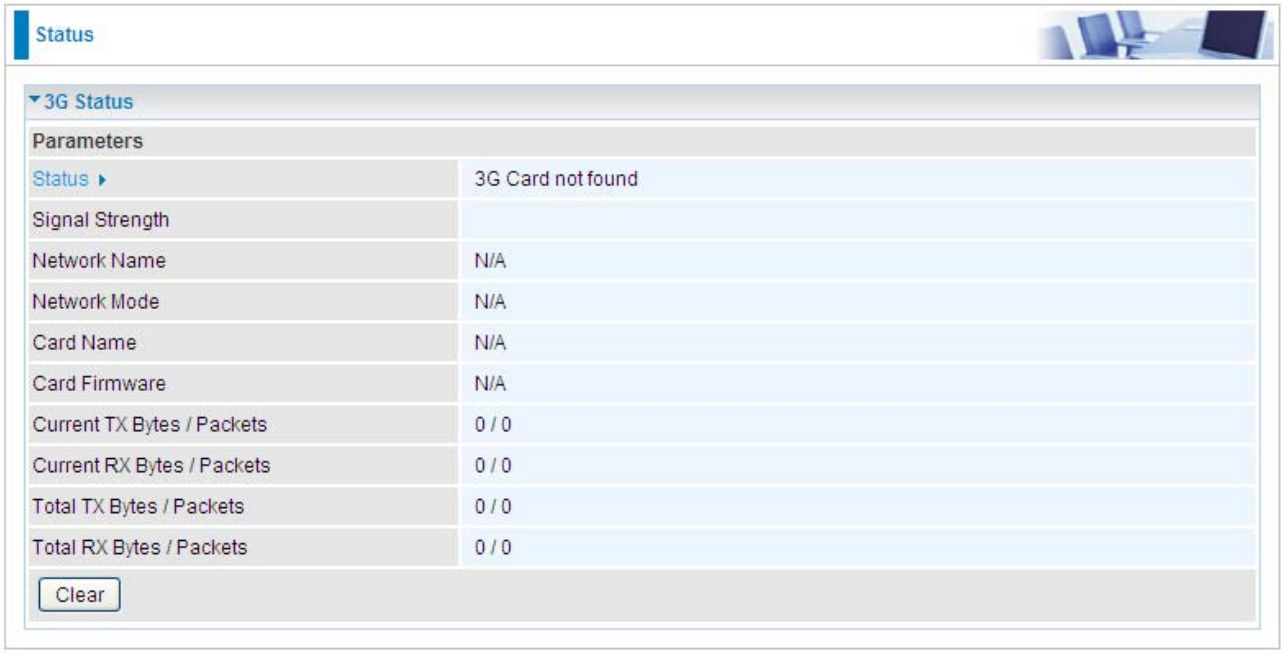


⊙ **ADSL Mode:** There are four modes “**Open Annex Type and Follow DSLAM’s Setting**”, ”**Annex A**”, ”**Annex L**”, ”**Annex M**” and **“Annex J”** that user can select for this connection.

⊙ **Modulator:** There are seven modes “**AUTO**”, ”**ADSL Multimode**”,”**ADSL2**”, ”**ADSL2+**”,”**G.Lite**”, “**T1.413**” and “**G.DMT**” that user can select for this connection.

- **Upstream:** Upstream rate.
- **Downstream:** Downstream rate.
- **SNR Margin (Upstream):** This is noise margin in upstream.
- **SNR Margin (Downstream):** This is noise margin in downstream.
- **Line Attenuation (Upstream):** This is attenuation of signal in upstream.
- **Line Attenuation (Downstream):** This is attenuation of signal in downstream.
- **Refresh:** Press this button to get the latest statistics.

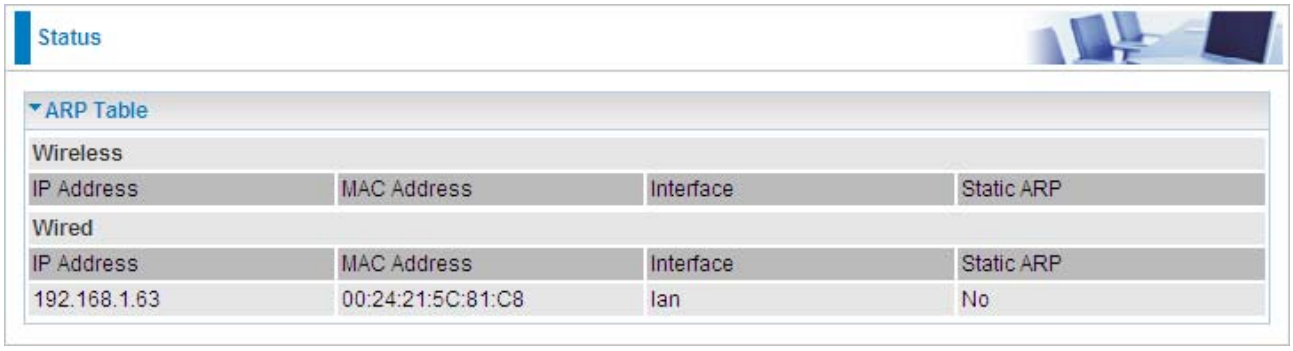
5.1.2 3G Status (BiPAC 7300NX only)



Status: The current status of the 3G card. Click **Status** to go to 3G configuration page.
Signal Strength: The signal strength bar indicates current 3G signal strength.
Network Name: The network name that the device is connected to.
Network Mode: The current operation mode in 3G card, it depends on service provider and card's limitation. It may be UMTS(3G), GPRS, EDGE, or GSM .
Card Name: The name of the 3G card.
Card Firmware: The current firmware for the 3G card.
Current TX Bytes / Packets: The statistics of transmission, count for this call.
Current RX Bytes / Packets: The statistics of receive, count for this call.
Total TX Bytes / Packets: The statistics of transmission, count from system ready
Total RX Bytes / Packets: The statistics of receive, count from system ready

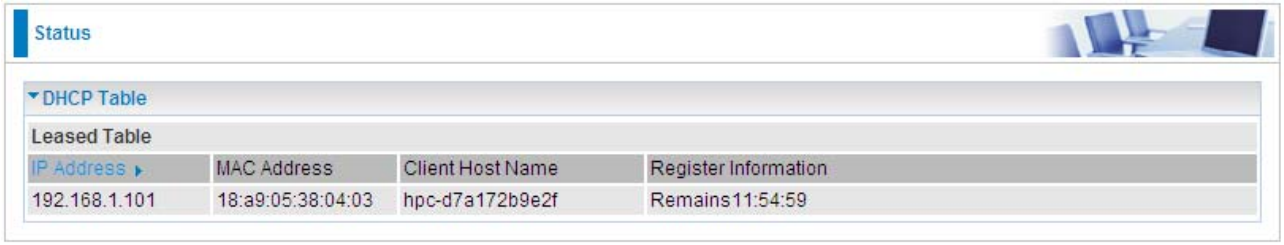
5.1.3 ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.



- **IP Address:** It is IP Address of internal host that join this network.
- **MAC Address:** The MAC address of internal host.
- **Interface:** The interface name (on the router) that this IP address connects to.
- **Static ARP:** Shows the status of static ARP.

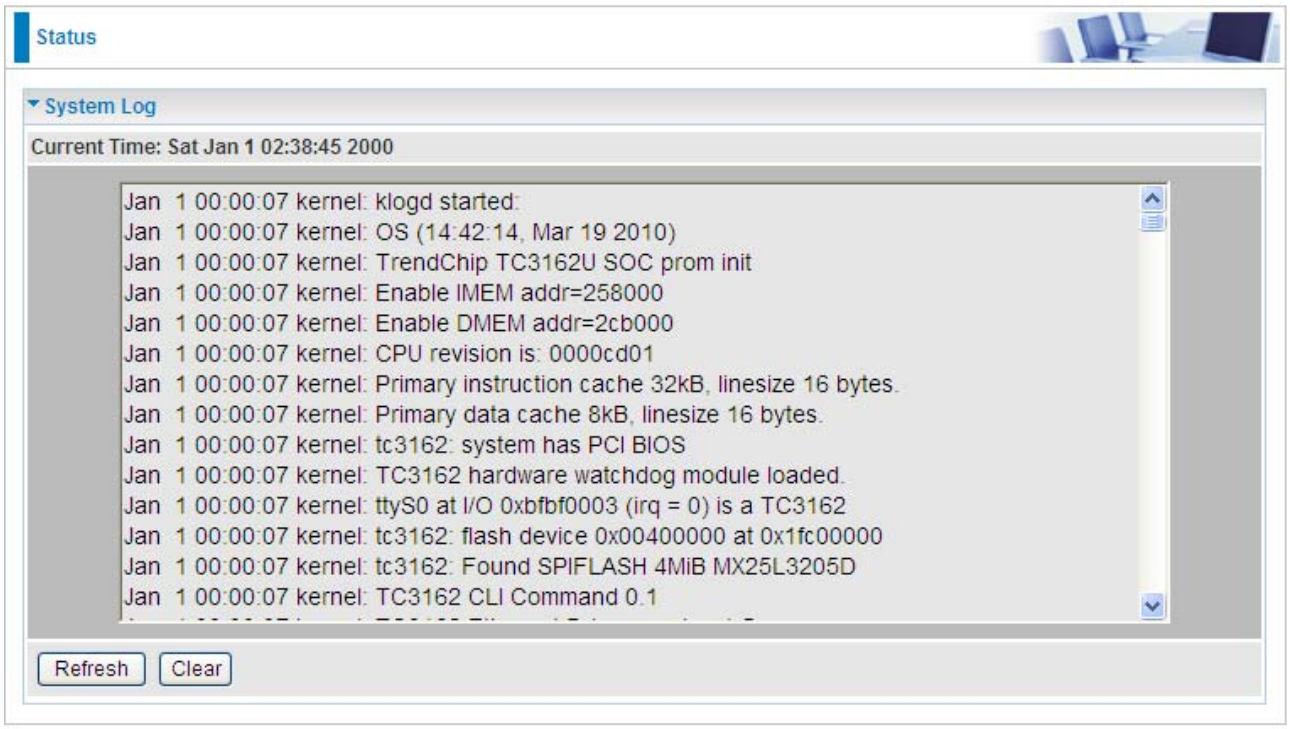
5.1.4 DHCP Table



- **IP Address:** The current corresponding DHCP-assigned dynamic IP address of the device.
- **MAC Address:** The MAC Address of internal DHCP client host.
- **Client Host Name:** The Host Name of internal DHCP client.
- **Register Information:** Register time information.

5.1.5 System Log

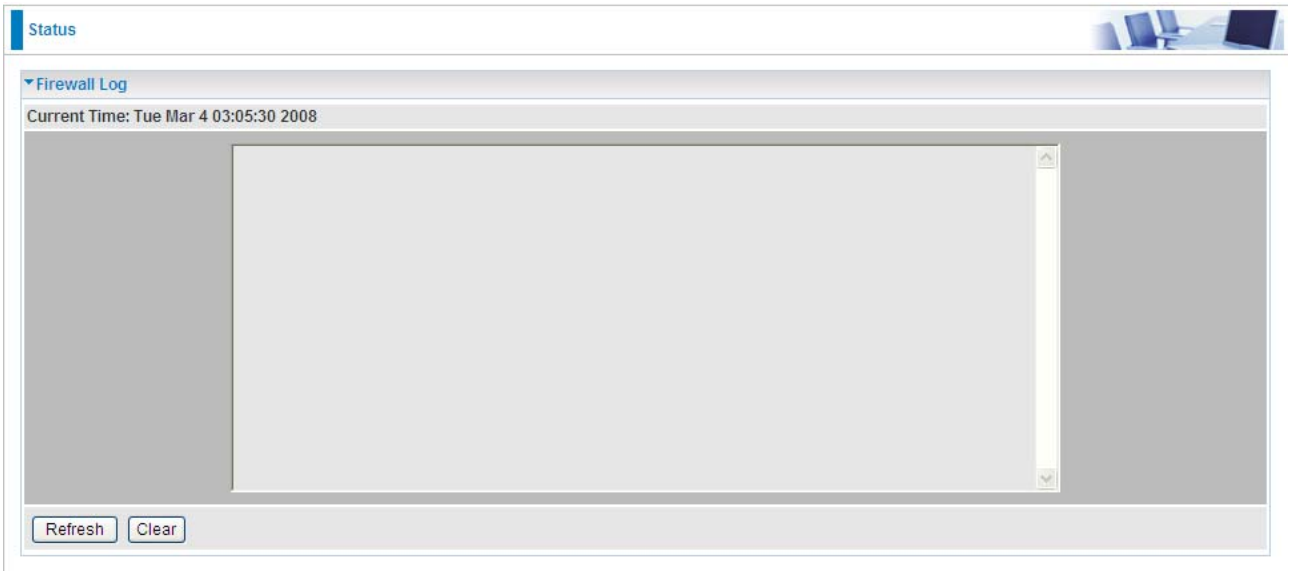
Display system logs accumulated up to the present time. You can trace historical information with this function.


Status
System Log
Current Time: Sat Jan 1 02:38:45 2000
Jan 1 00:00:07 kernel: klogd started:
Jan 1 00:00:07 kernel: OS (14:42:14, Mar 19 2010)
Jan 1 00:00:07 kernel: TrendChip TC3162U SOC prom init
Jan 1 00:00:07 kernel: Enable IMEM addr=258000
Jan 1 00:00:07 kernel: Enable DMEM addr=2cb000
Jan 1 00:00:07 kernel: CPU revision is: 0000cd01
Jan 1 00:00:07 kernel: Primary instruction cache 32kB, linesize 16 bytes.
Jan 1 00:00:07 kernel: Primary data cache 8kB, linesize 16 bytes.
Jan 1 00:00:07 kernel: tc3162: system has PCI BIOS
Jan 1 00:00:07 kernel: TC3162 hardware watchdog module loaded.
Jan 1 00:00:07 kernel: ttyS0 at I/O 0xbfbf0003 (irq = 0) is a TC3162
Jan 1 00:00:07 kernel: tc3162: flash device 0x00400000 at 0x1fc00000
Jan 1 00:00:07 kernel: tc3162: Found SPIFLASH 4MiB MX25L3205D
Jan 1 00:00:07 kernel: TC3162 CLI Command 0.1
Refresh
Clear

5.1.6 Firewall Log

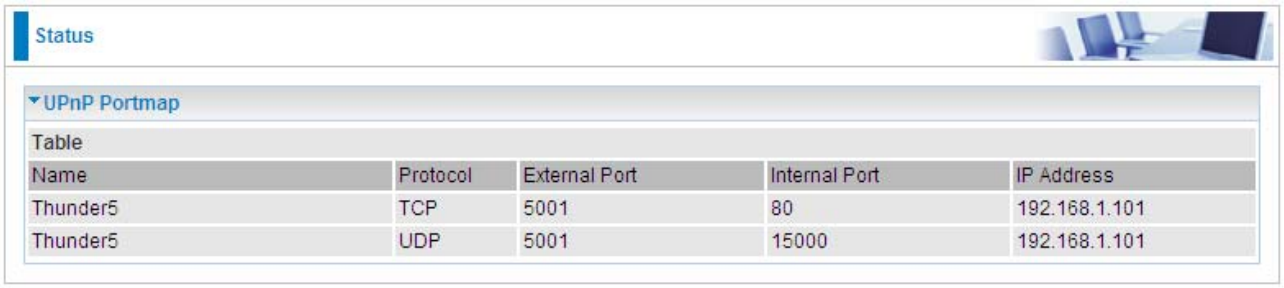
Firewall Log displays log information of any unexpected action with your firewall settings.

This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



5.1.7 UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the Advanced section of this manual for more details on UPnP and the router's UPnP configuration options.

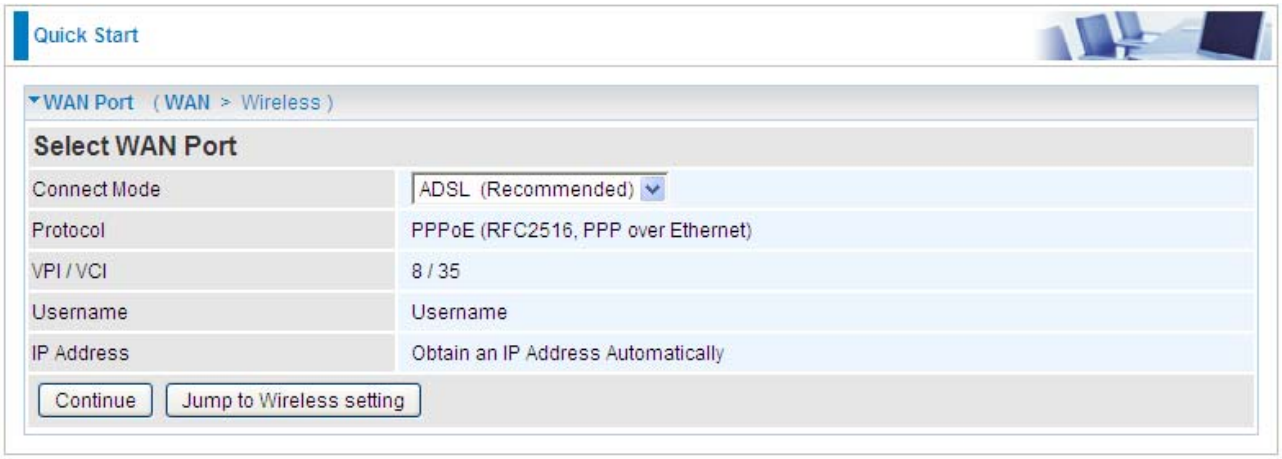


- **Name:** the description of this application.
- **Protocol:** the protocol used by UpnP NAT Mapping.
- **External Port:** the external service port transformed by the mapping，thus the remote port or the port in the WAN wanting to connect in.
- **Internal Port:** the internal service port.
- **IP Address:** the internal host IP address.

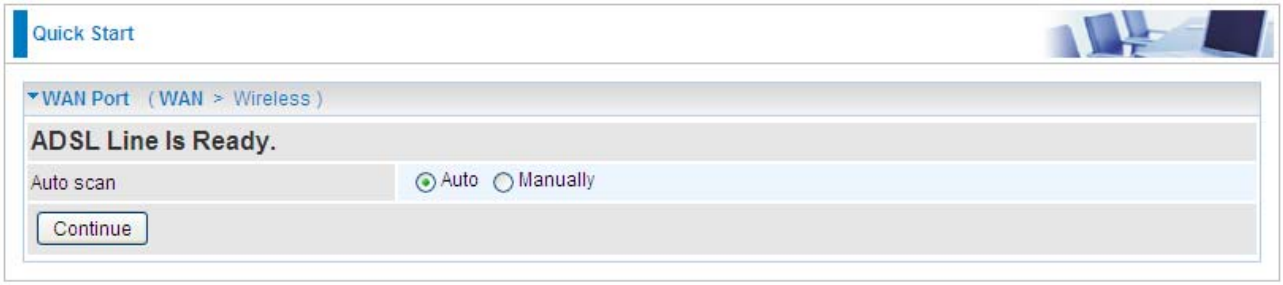
5.2 Quick Start

ADSL

Step1: select ADSL connection Mode. Click **Continue** to go to next step.

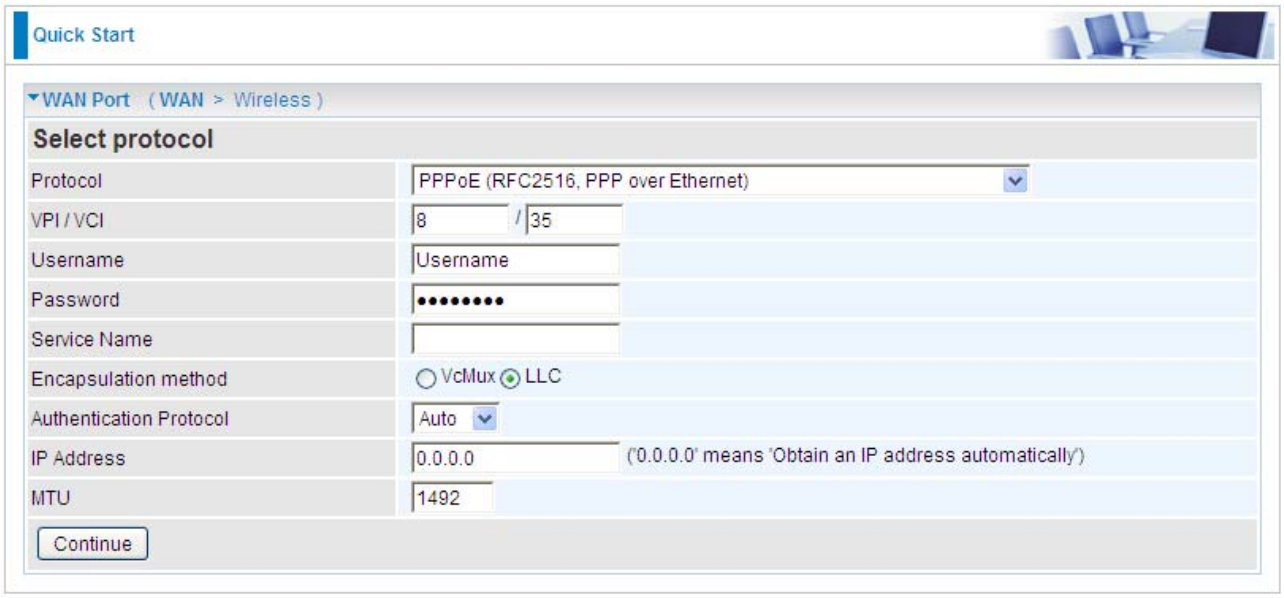


Step2: select Auto to let this device to automatically scan the VPI/VCI, go to step 3. Or select Manually to go to step 4.



Step 3: wait when the ADSL is scanning. Also you can **Abort to manually setting** and go to next step 4.

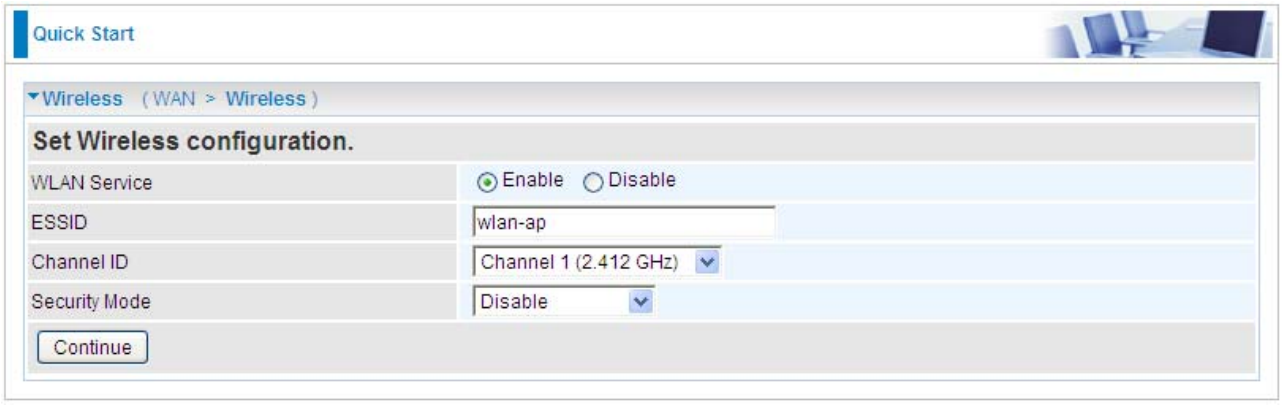
Step 4: type the username and password provided by your ISP. Click Continue to go on.



Step 5: wait while the device is configured.

Step 6: WAN connection configuration is successful.

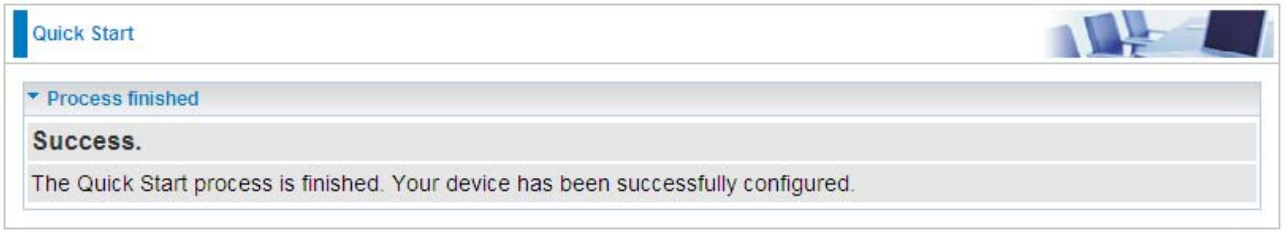
Step 7: Click Next to Wireless to do wireless configuration.



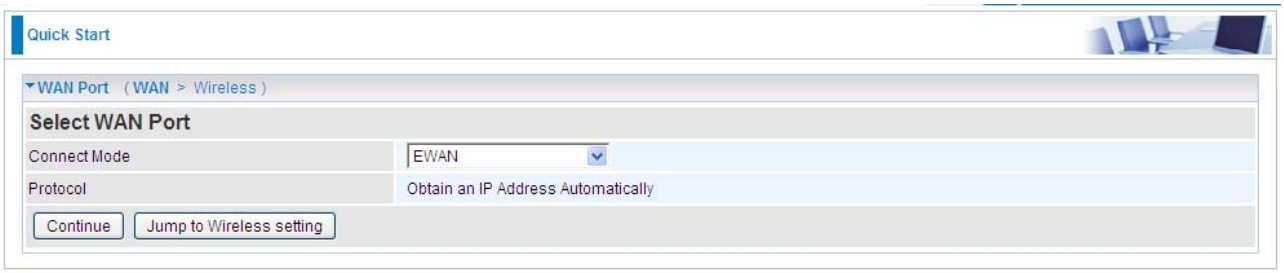
Enter the ESSID, select the Channel ID and the Security Mode, click **Continue** to go on. For detail, please turn to **WLAN** in this manual for help.

Step 8: wait while saving configuration to Flash.

Step 9: success.


Quick Start
Process finished
Success.
The Quick Start process is finished. Your device has been successfully configured.

EWAN (BiPAC 7300N *RE* only)



Click on **Continue** to choose the Protocol to connect with EWAN or click **Jump to Wireless Setting** to use Protocol: Obtain an IP Address Automatically to connect and setup wireless settings at the same time.

Obtain an IP Address Automatically

When connecting to the ISP, BiPAC 7300N *RE* also functions as a DHCP client. BiPAC 7300N *RE* can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.

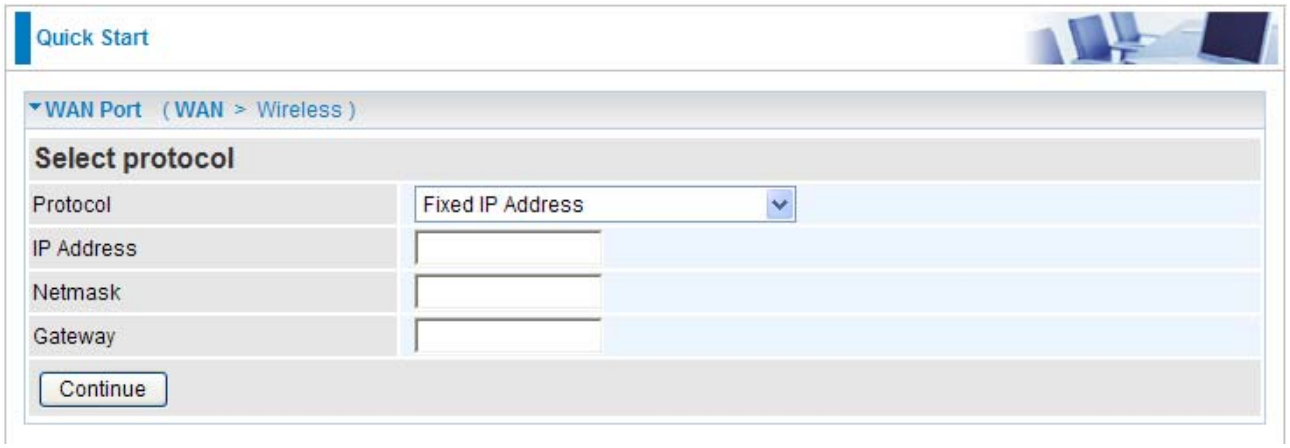
Protocol: The current ATM protocol in the device

Click on the **Continue** button and wait for your connection to be connected.

If connection is successful the following image will be shown.

Fixed IP Address

Select this option to set static IP information. You will need to enter in the Connection type, IP address, Netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



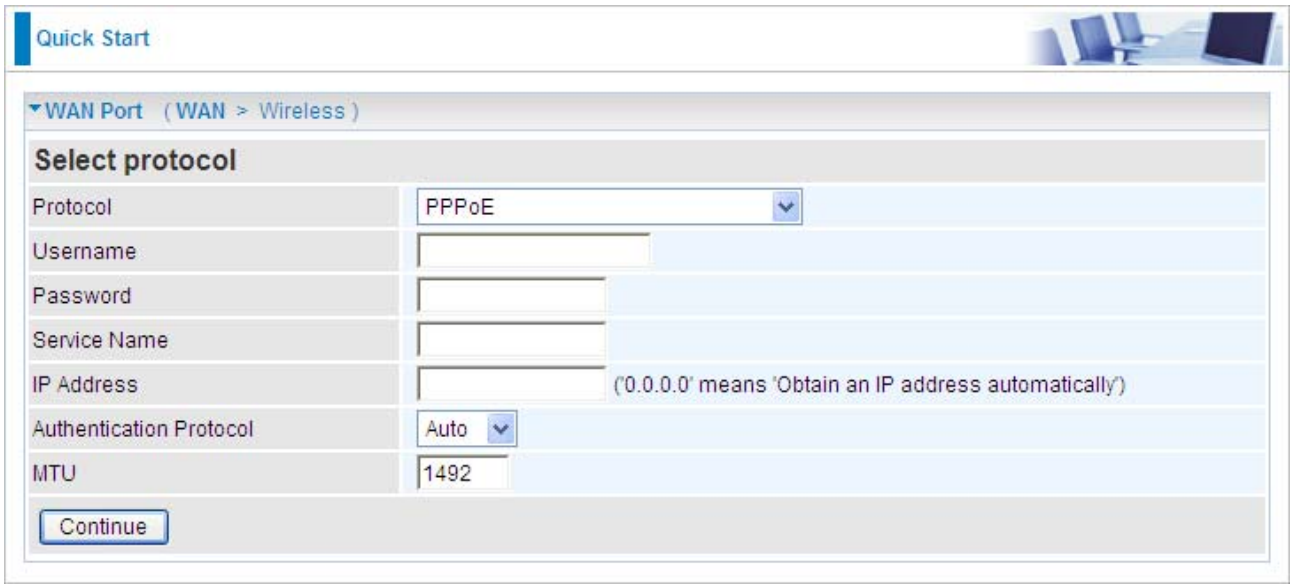
- **Protocol:** The current ATM protocol in the device
- **IP Address:** Enter your WAN IP address.
- **Netmask:** Type the subnet mask assigned to you by your ISP (if given).
- **Gateway:** You must specify a gateway IP address (supplied by your ISP)

Click on the **Continue** button and wait for your connection to be connected.

If connection is successful the following image will be shown.

PPPoE

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.

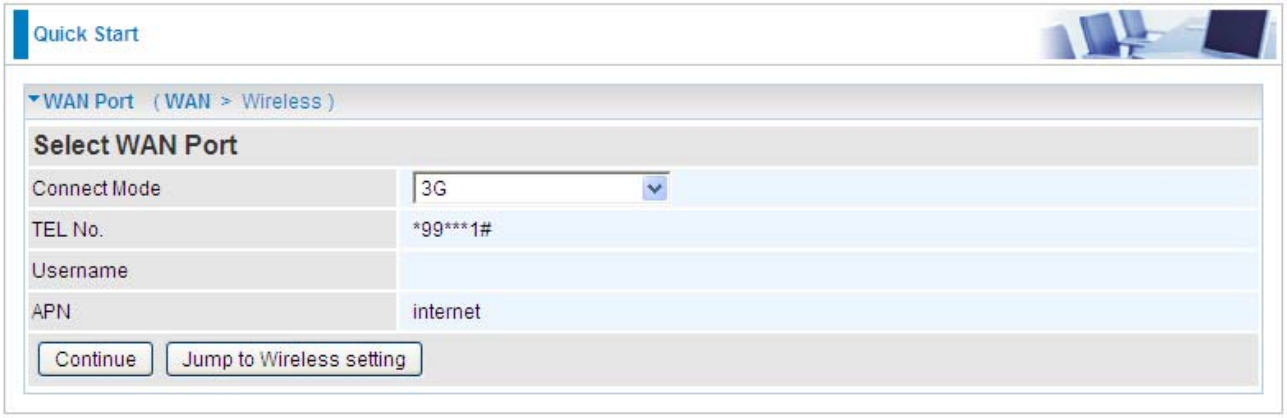


- **Protocol:** The current ATM protocol in the device
- **Username:** Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).
- **Service Name:** Enter a name for this connection.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Auth. Protocol:** Default is Auto. Your ISP advises on using Chap or Pap.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Click on the **Continue** button and wait for your connection to be connected.

If connection is successful the following image will be shown.

3G (BiPAC 7300NX only)



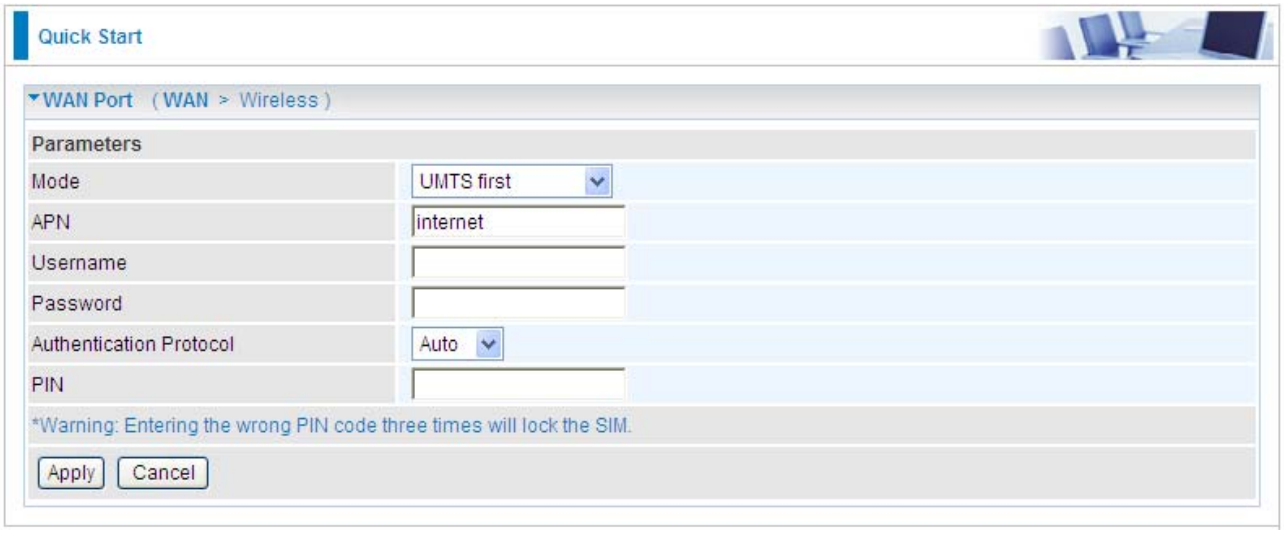
Connect Mode: 3G.

TEL No.: The dial string to make a GPRS / 3G user internetworking call.

Username: The username provided by your service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call.

Click **Continue** to go to next step.



Mode: There are 5 options of phone service standards: GSM only, UTMS only, GPRS/EDGE first, UMTS first, and Automatic. If you are uncertain what services are available to you, and then please select Automatic.

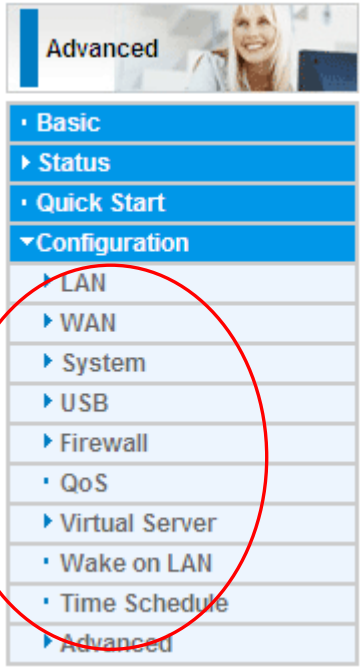
APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. Some 3G operators use the APN ‘internet’ for their portal. The default value is “internet”.

Username/Password: Enter the username and password provided by your ISP.
Authentication Protocol: Default is Auto. Please consult your ISP on whether to use PAP, CHAP.
PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

5.3 Configuration

Click this item to access the following sub-items that configure the ADSL router: **LAN, WAN, System, USB (BiPAC 7300NX only), Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule** and **Advanced.**

These functions are described in the following sections.



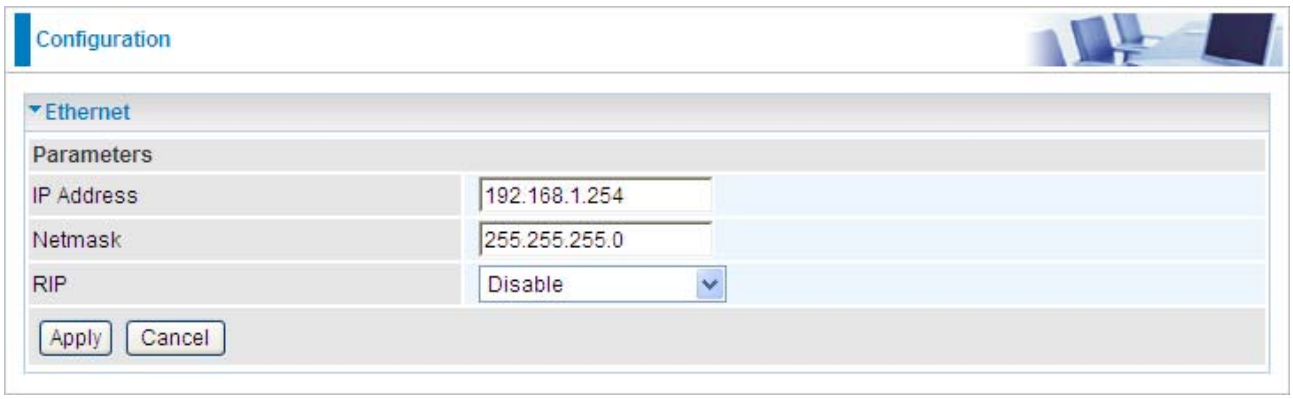
(BiPAC 7300NX)

5.3.1 LAN (Local Area Network)

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

There are six items within the LAN section: **Ethernet, IP Alias, Wireless, Wireless Security, WPS** and **DHCP Server**.

5.3.1.1 Ethernet

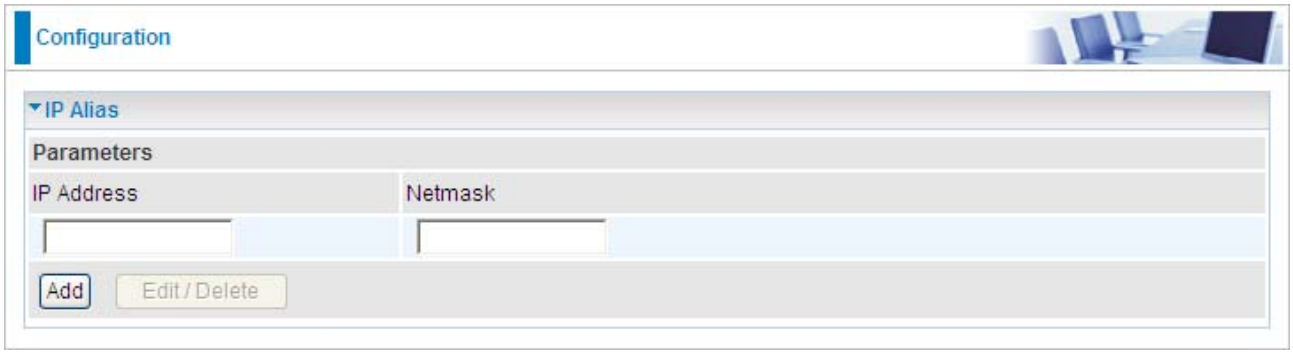


The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.

- **IP Address:** The default IP on this router.
- **Netmask:** The default subnet mask on this router.
- **RIP:** RIP v1, RIP v2 Broadcast, RIP v1+v2 Broadcast and RIP v2 Multicast.

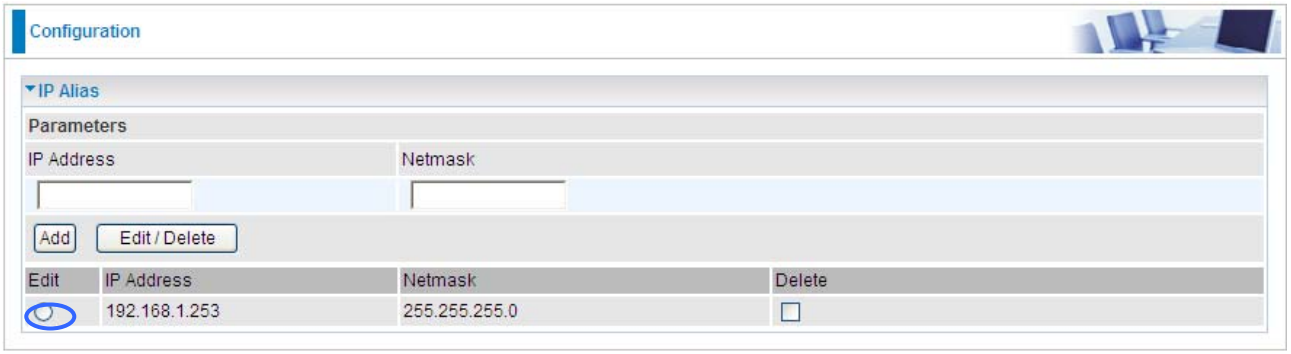
5.3.1.2 IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.

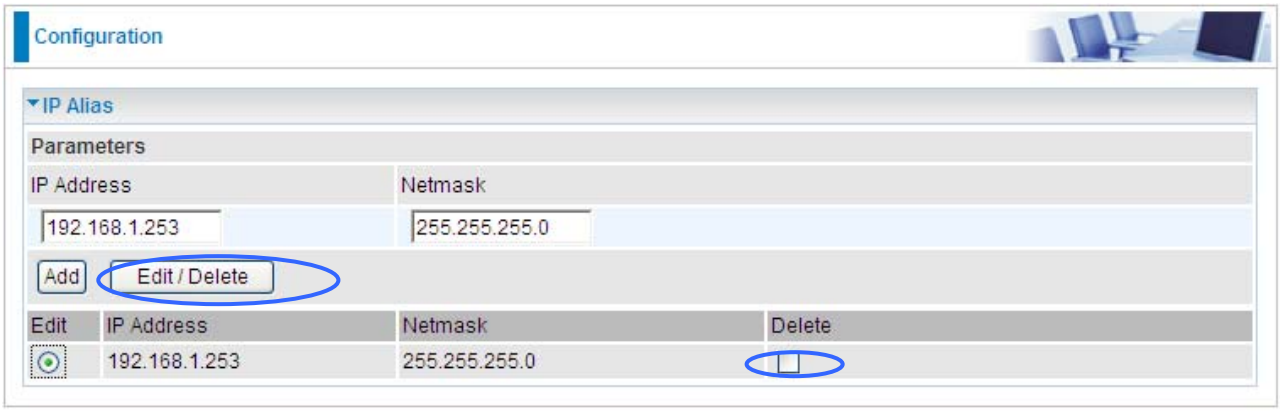


- **IP Address:** Specify an IP address on this virtual interface.
- **Netmask:** Specify a subnet mask on this virtual interface.

Press Add to apply and the corresponding information will be listed below.



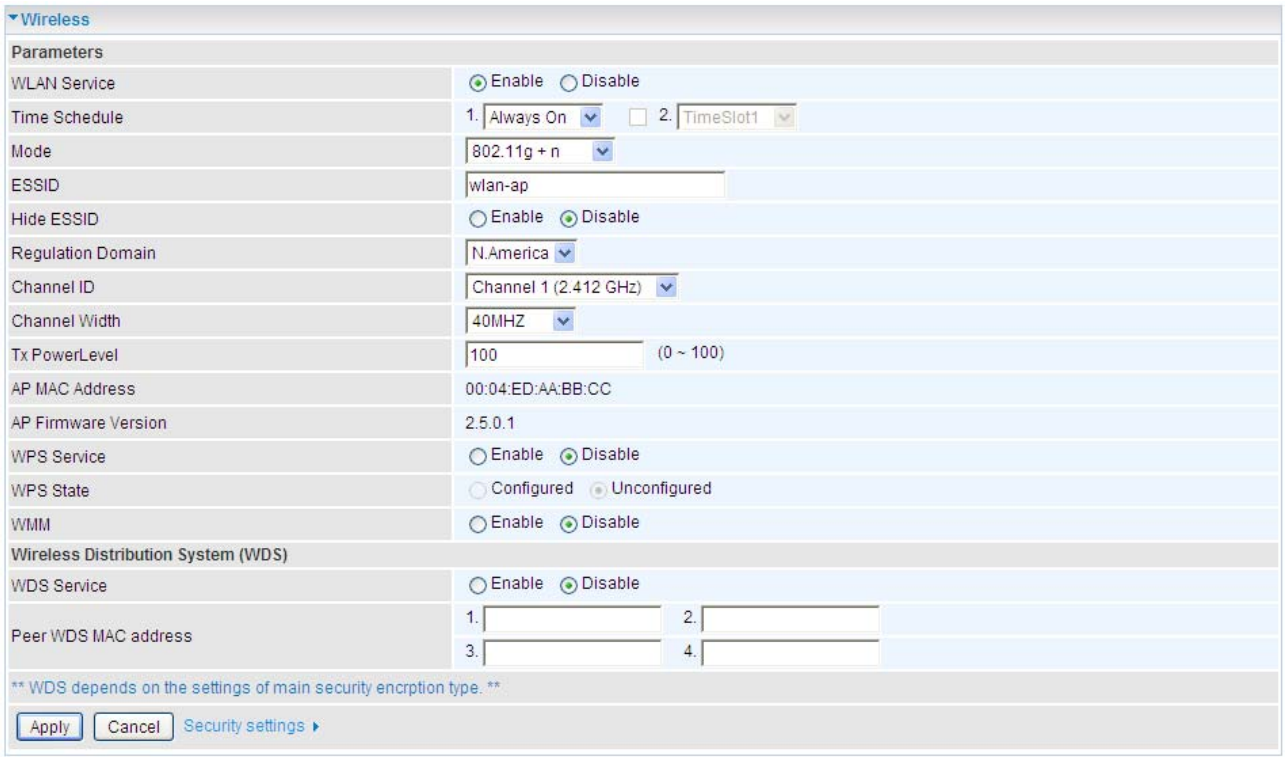
Click **Edit** radio button, then the item you want to reedit will be displayed above just as showed below.



Press **Edit/Delete** to apply your modification.

Check **Delete** if you want to delete the item, then press **Edit/Delete**, the deleting prompt window will appear to remind you, do as you like.

5.3.1.3 Wireless



Parameters

- **WLAN Service:** Default setting is set to **Enable**.
- **Time Schedule:** A self-defined time period. You may specify a time schedule for your

prioritization policy.

Here we provide two groups of **Time Schedule** setting. You can flexibly set the time you want the wireless connection works.

If you select **Always On** in group1, then the group2 is disabled.

While if you select any other item from the group1 drop-down menu, the group2 will be activated. Select the timeslot you want, then the wireless will work according to the time of the two time schedule settings. That is to say you can flexibly set the time the wireless works.

For example, if you select TimeSlot1 in group1, then the group2 is activated, you can select a timeslot from the drop-down menu, then the wireless connection will perform according to the two timeslots you have set.

For setup and detail**,** refer to **Time Schedule** section.

Mode: The default setting is **802.11g+n** (Mixed mode). If you do not know or have both 11g and 11n devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **802.11g** if you have only 11g card. If you have only 11b card, then select **802.11b**. If you have only 11n card, then select **802.11n**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable.**

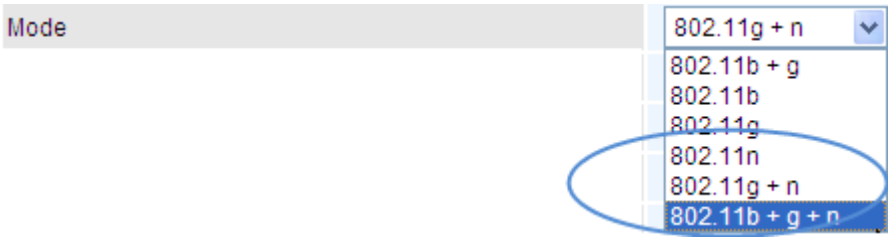
⊙ **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hided in stead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.

⊙ **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

- **Channel ID:** Select the ID channel that you would like to use.
- **Channel Wdith:** Select either **20 MHz** or **20/40 MHz** or **40MHZ** for the channel bandwidth. The higher the bandwidth the better the performance will be.

Note: This parameter appears only when you select one of the item as the following graph



- **Tx Power Level:** It is function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: The Power Level maybe different in each access network user premises environment and choose the most suitable level for your network.

- **AP MAC Address:** It is a unique hardware address of the Access Point.
- **AP Firmware Version:** The Access Point firmware version.
- **WPS service:** Enable / disable
- **WPS State:** Current WPS state in AP. It is be used for WCN (Windows Connect Now).
  - **Configured:** This AP is be configured via WPS. It is not allowed to configure via WCN.
  - **Unconfigured:** This AP is un-configured via WPS. It can be configured via WCN.

WMM: This feature works concurrently with QoS that enables the system to prioritize the flow of data packets according to 4 categories: Voice, Video, Best Efforts and Background.

- **Enable:** Check to activate WMM feature.
- **Disable:** Check to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, simply define the peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

- **WDS Service:** The default setting is **Disable.** Check **Enable** radio button to activate this function.

- **1. Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.

- **2. Peer WDS MAC Address:** It is the second associated AP's MAC Address.
- **3. Peer WDS MAC Address:** It is the third associated AP's MAC Address.
- **4. Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

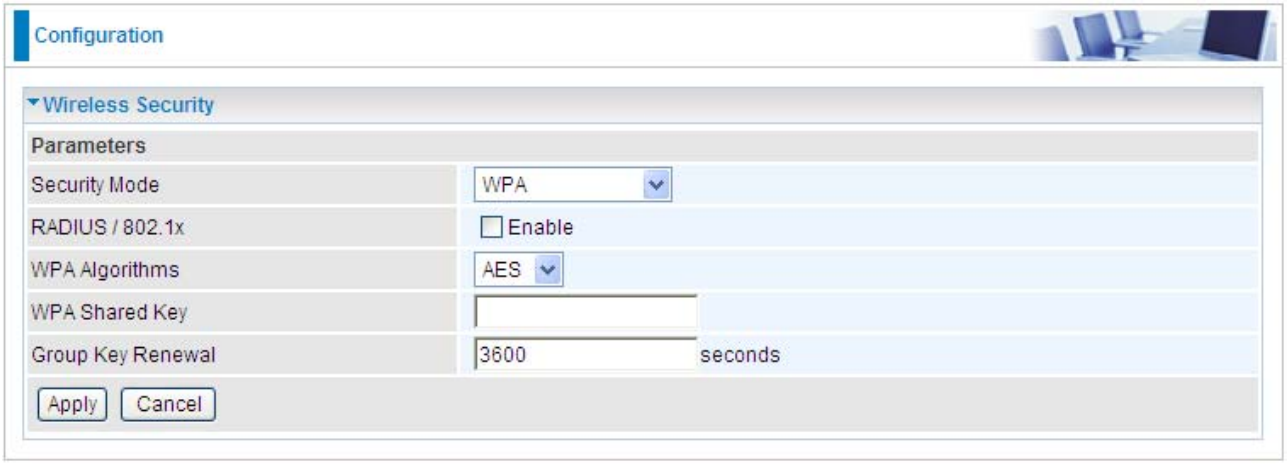
Note: For MAC Address, Semicolon (:) or Dash (-) must be included.

5.3.1.4 Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA or WPA2

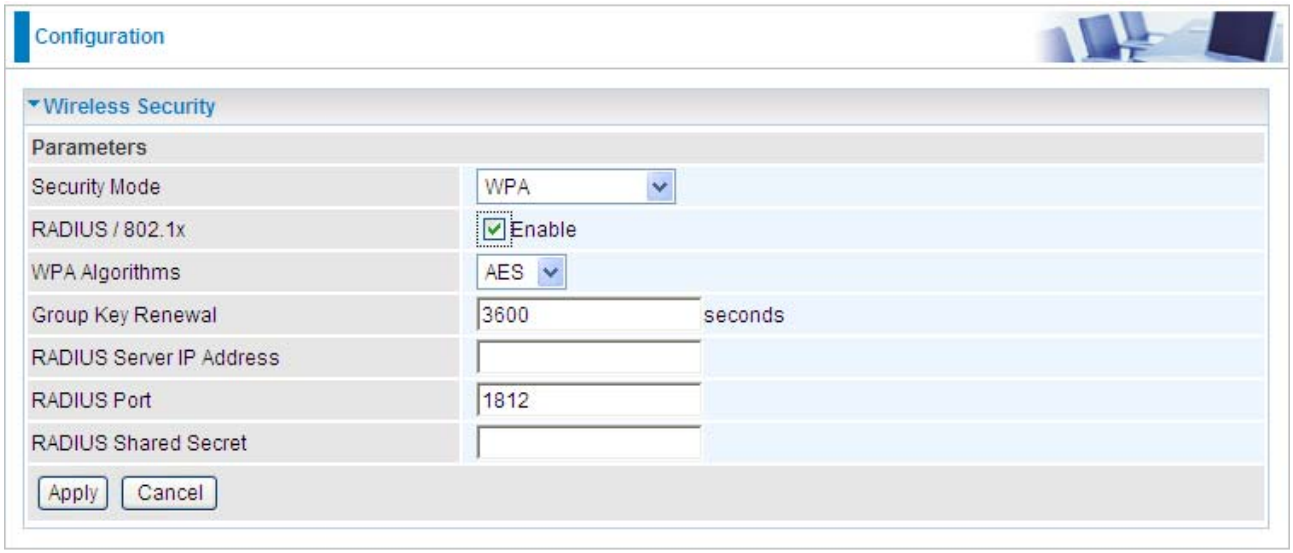
Here take **WPA** for example.



- **Security Mode:** You can choose the type of security mode you want to apply from the drop down menu.
- **RADIUS/802.1x:** Whether to enable RADIUS function or not (For WPA/WPA2/WEP encryption).
- **WPA Algorithms:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication. The Default algorithms is AES.
- **WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Group Key Renewal:** The period of renewal time for changing the security key

automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

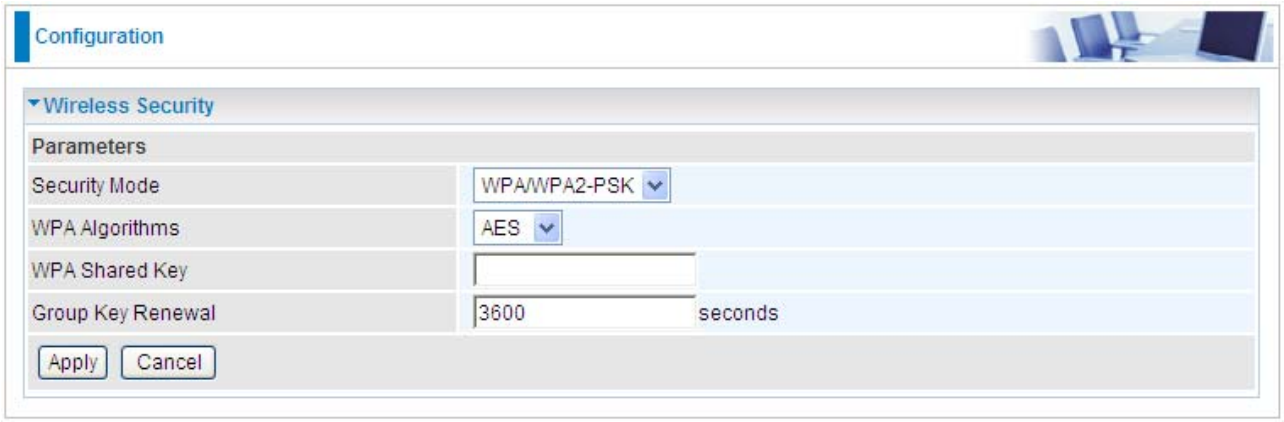
If you want to enable the RADIUS service, check Enable and then do the following settings.



- **RADIUS Server IP Address:** Enter the IP address of RADIUS authentication server.
- **RADIUS Server Port:** Enter the port number of RADIUS authentication server here. Default value is 1812.
- **RADIUS Shared Secret:** Enter the password of RADIUS authentication server.

Click Apply to confirm the settings.

WPA / WPA2 - PSK



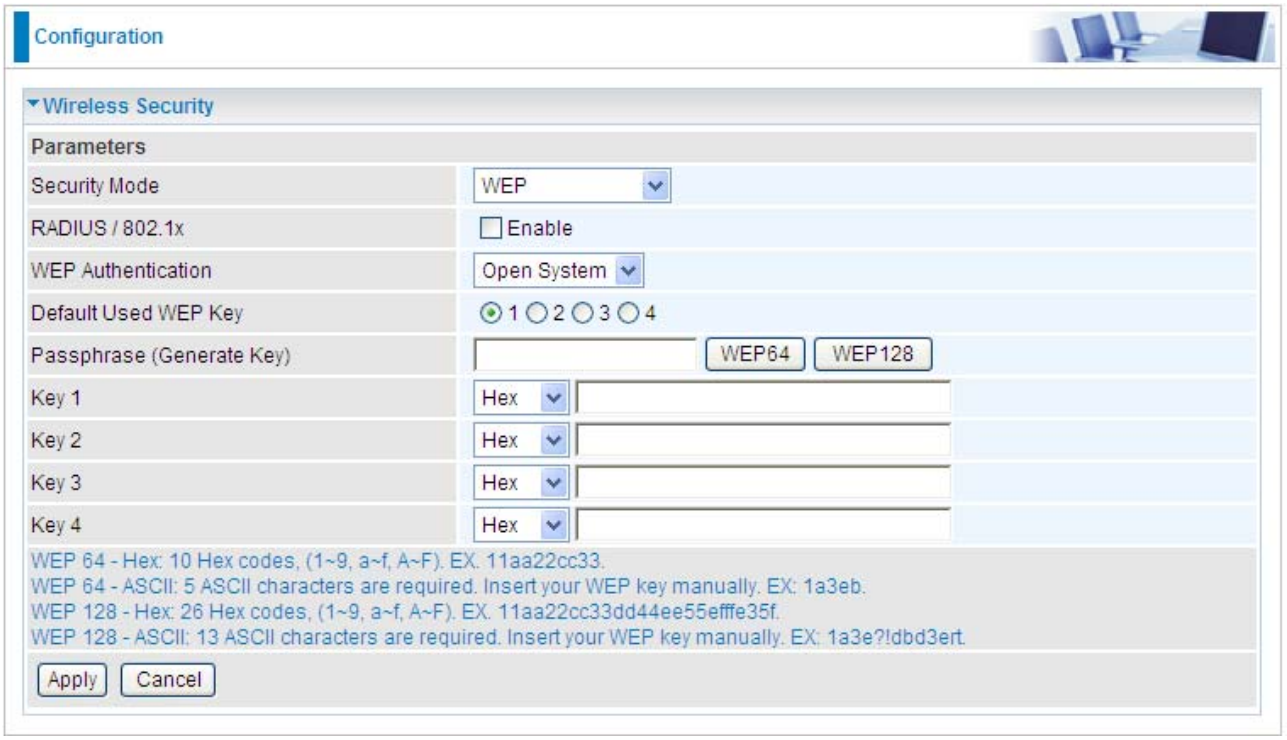
- **Security Mode:** You can choose the type of security mode you want to apply from the drop-down menu.
- **WPA Algorithms:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

The Default algorithm is AES.

- **WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

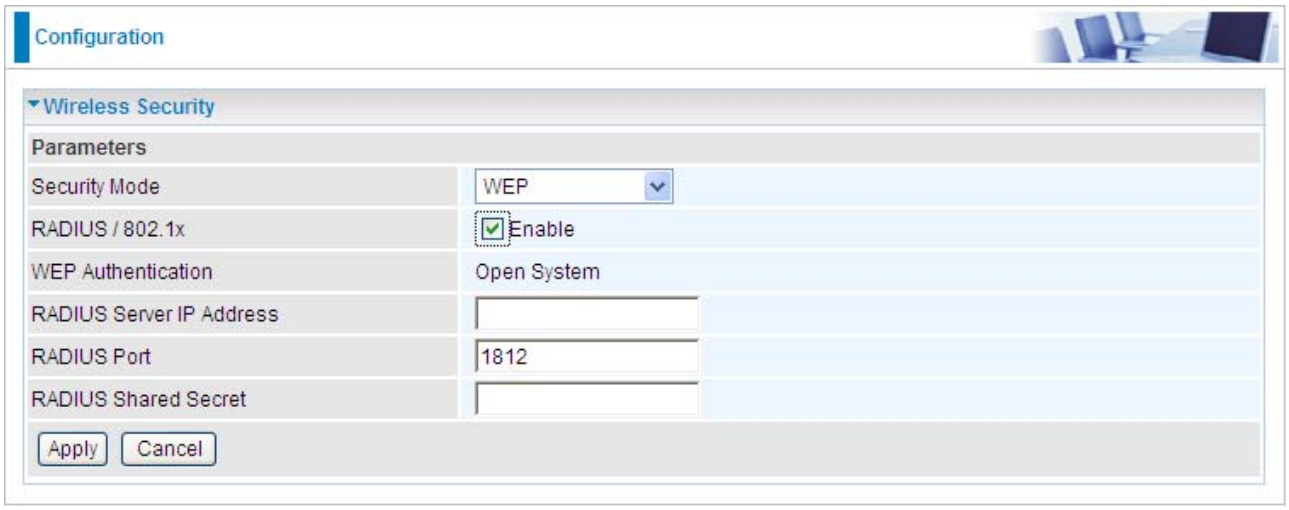
Click Apply to confirm the settings.

WEP



- **RADIUS / 802.1x:** Whether to enable RADIUS / 802.1x.
- **WEP Authentication:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. There are 3 options to select from: **Open System, Shared key** or **both**.
- **Default Used WEP Key:** Select the encryption key ID; please refer to **Key (1~4)** below.
- **Passphrase:** This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.
- **Key (1-4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be either HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS service, check Enable and then do the following settings.



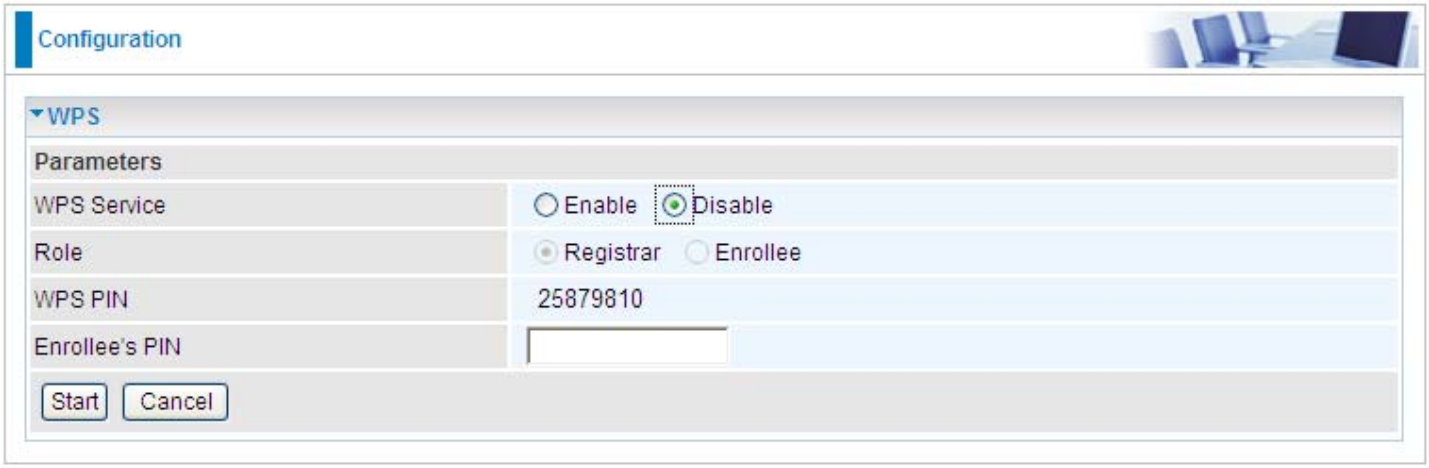
- **WEP Authentication:** If you enable **RADIUS/802.1x,** then the default **WEP Authentication** is **Open System.**
- **RADIUS Server IP Address:** Enter the IP address of RADIUS authentication server.
- **RADIUS Server Port:** Enter the port number of RADIUS authentication server here. Default value is 1812.
- **RADIUS Shared Secret:** Enter the password of RADIUS authentication server.

Click Apply to confirm the settings.

Note: *For information about settling Radius/802.1x, please refer to* WLAN *setup section.*

5.3.1.5 WPS

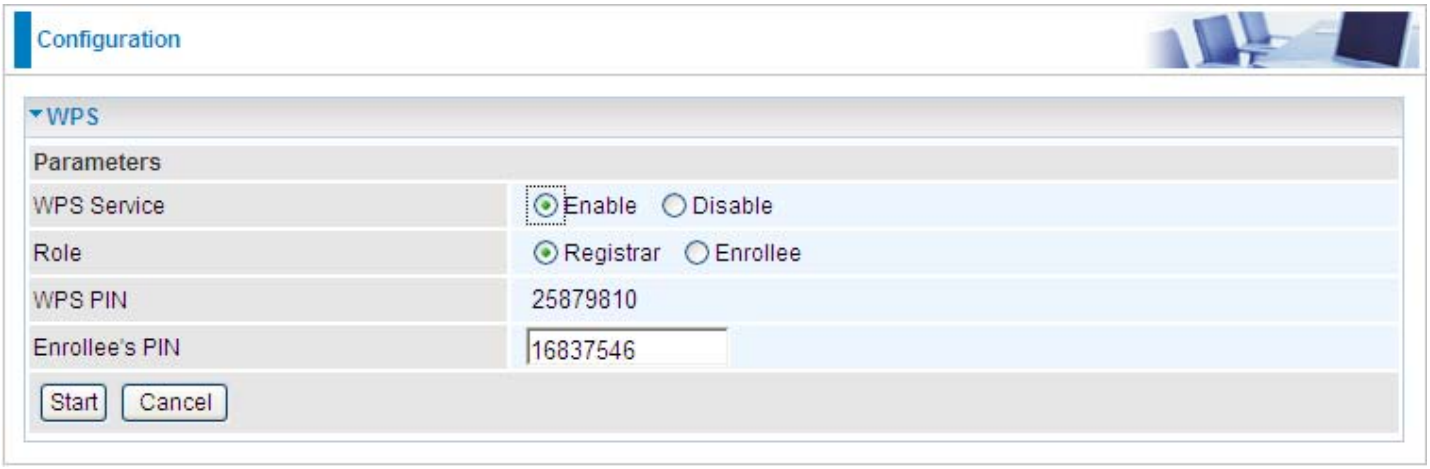
WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.



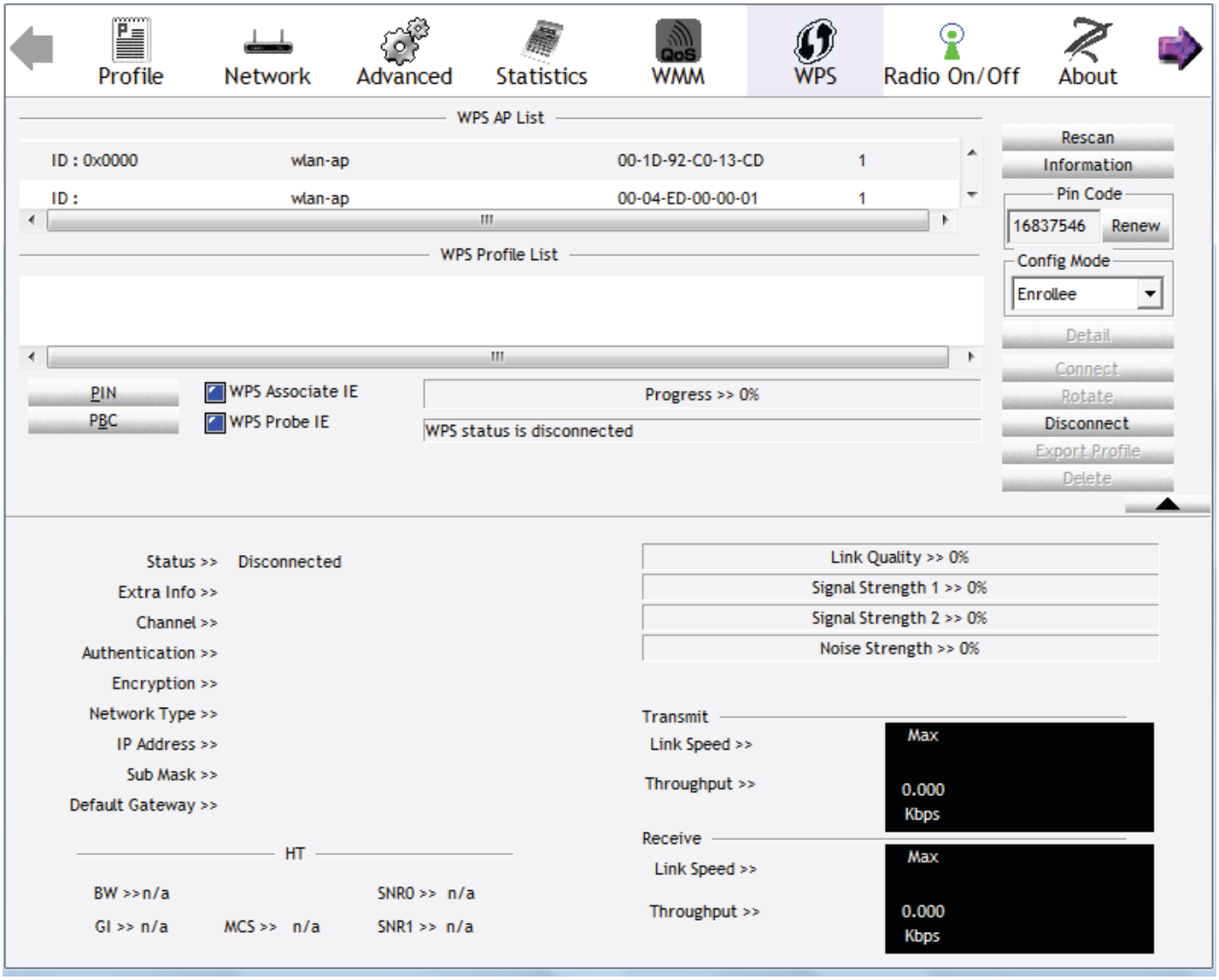
Wi-Fi Network Setup

PIN Method: Configure AP as Registrar

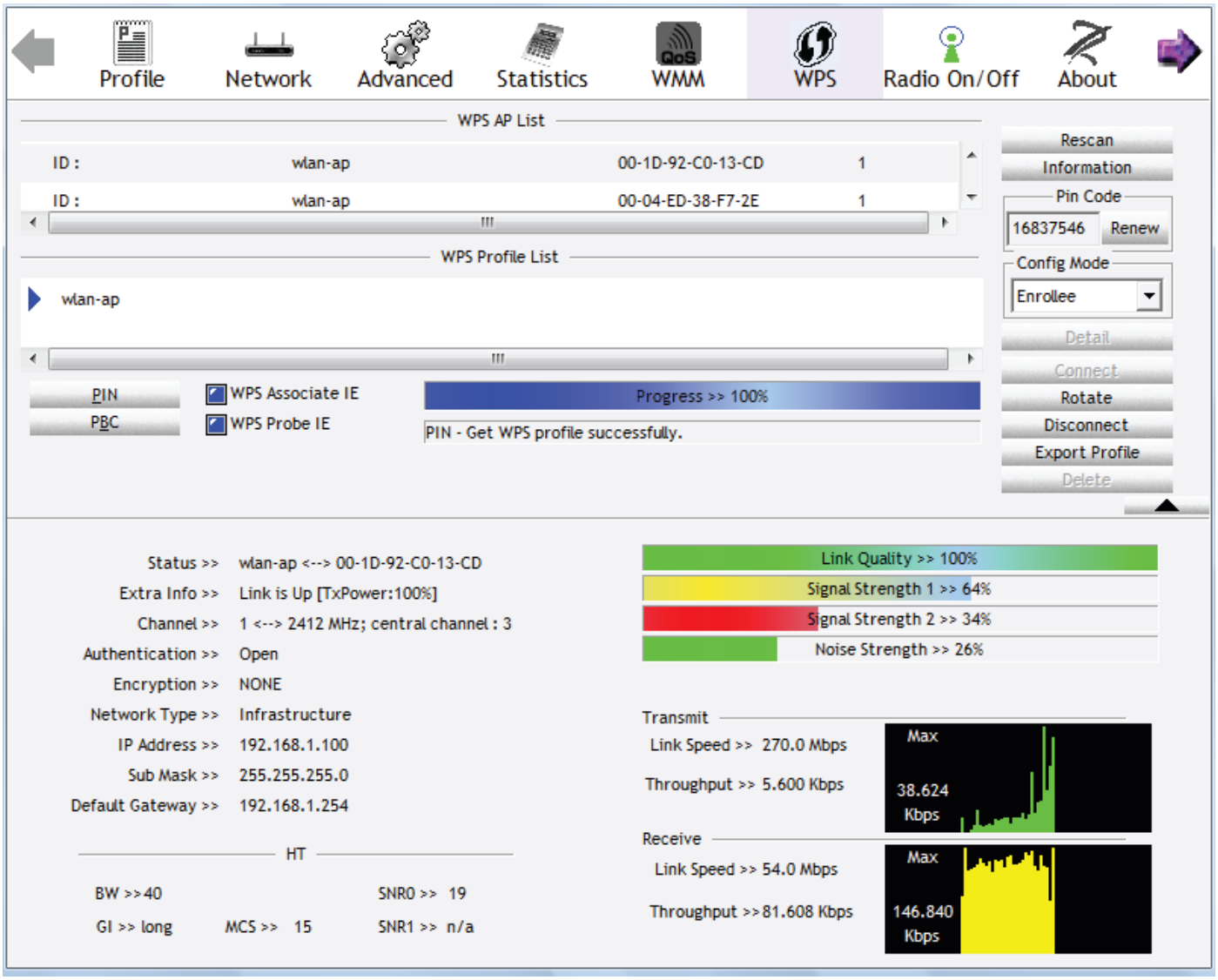
1. Jot down the client's Pin (eg. 16837546).
2. Enter the Enrollee's PIN number and then press Start.



3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

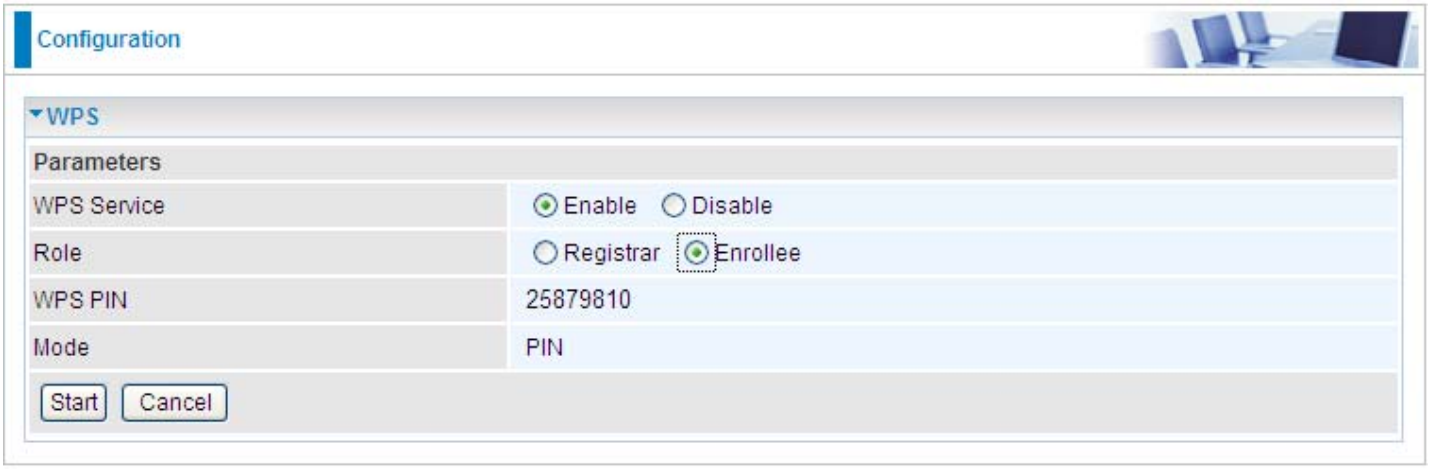


4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.

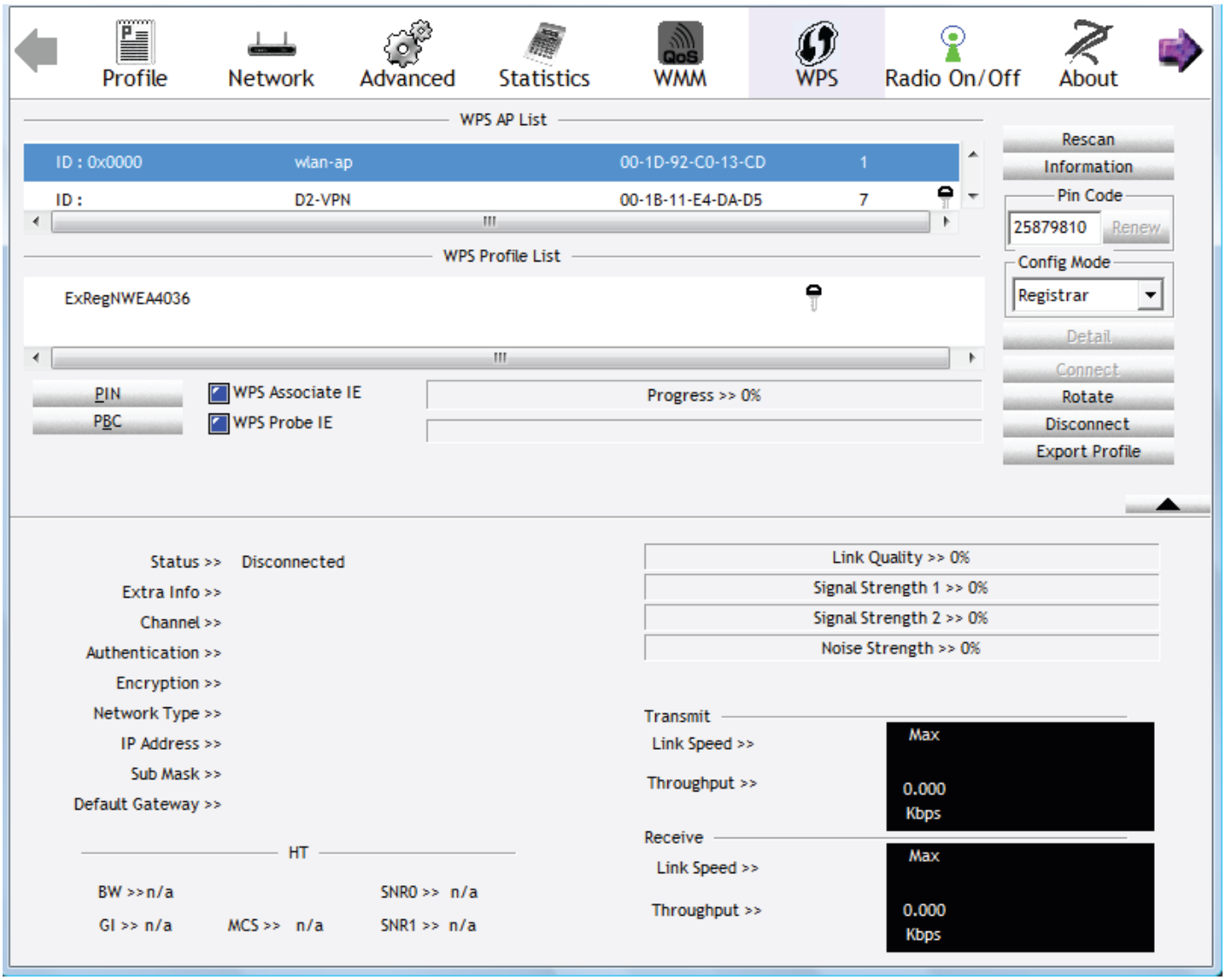


PIN Method: Configure AP as Enrollee

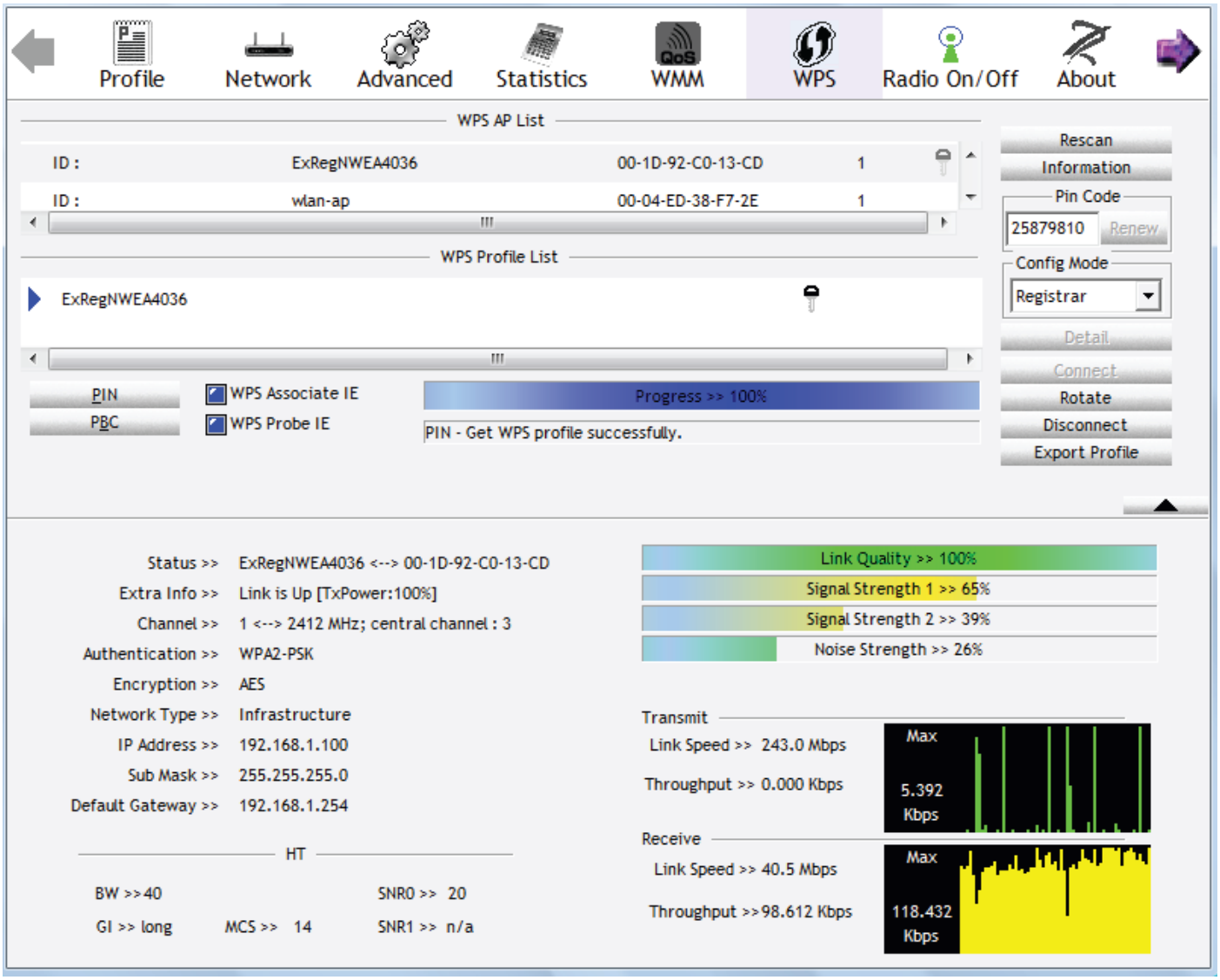
1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (eg. 25879810).



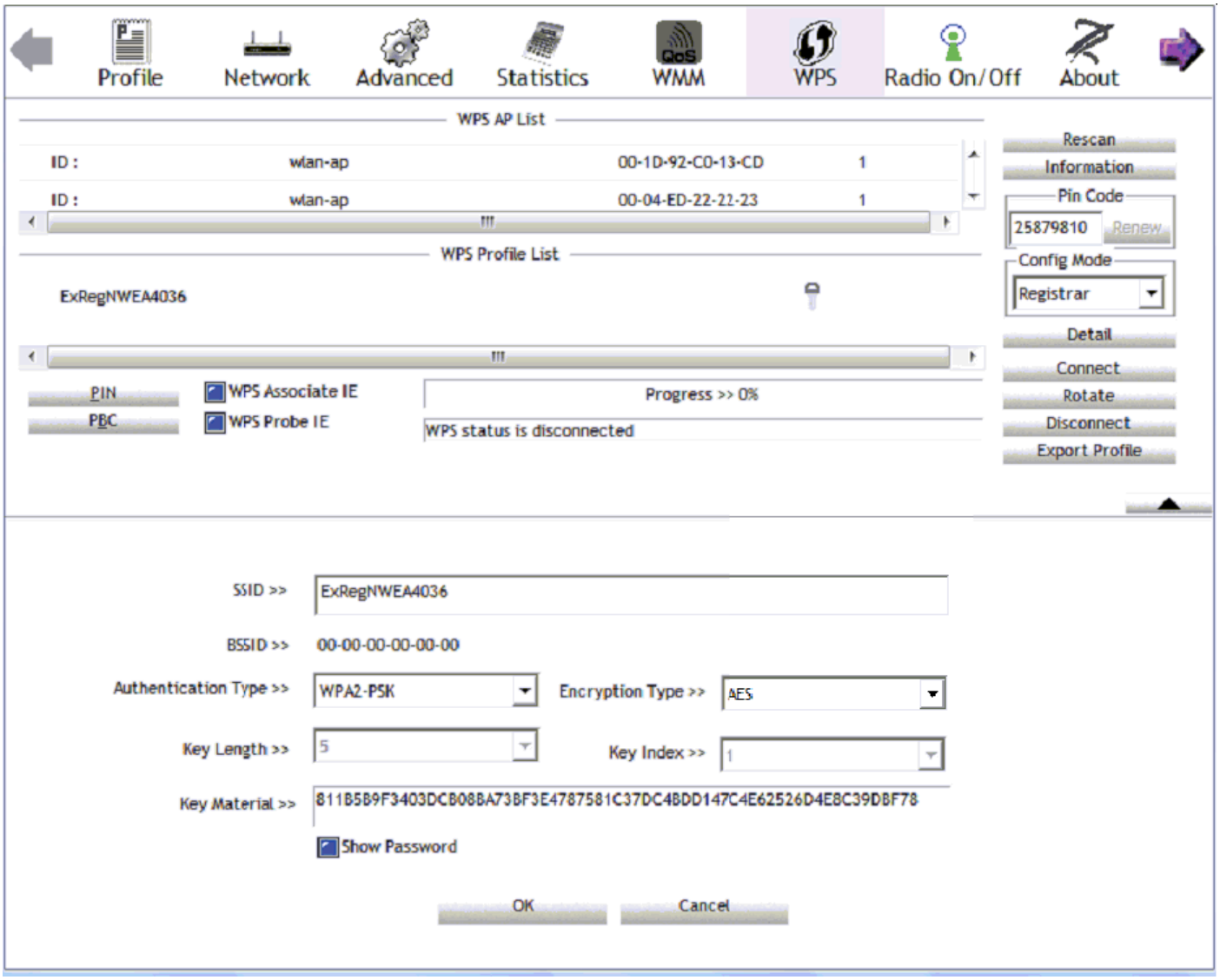
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.



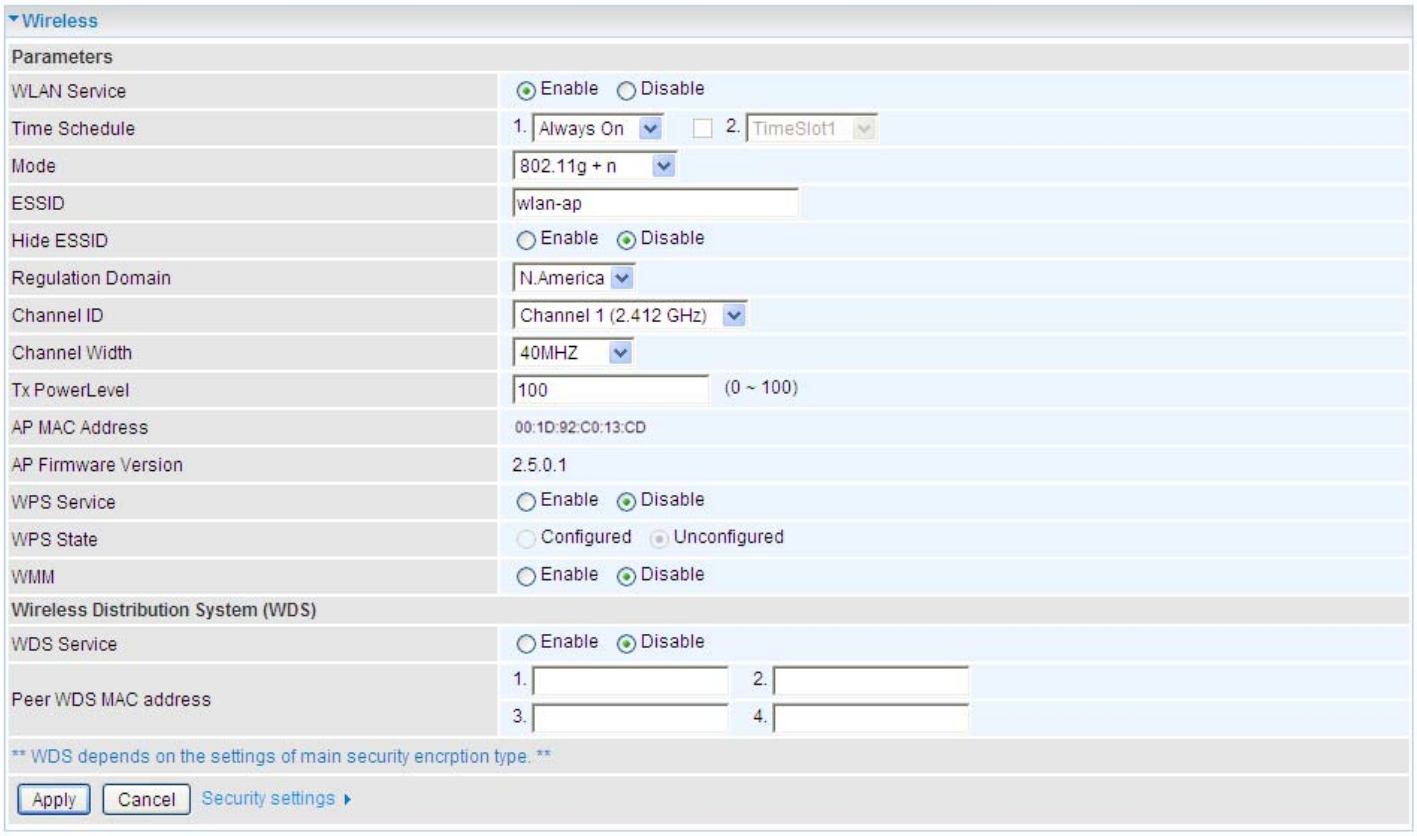
4. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.

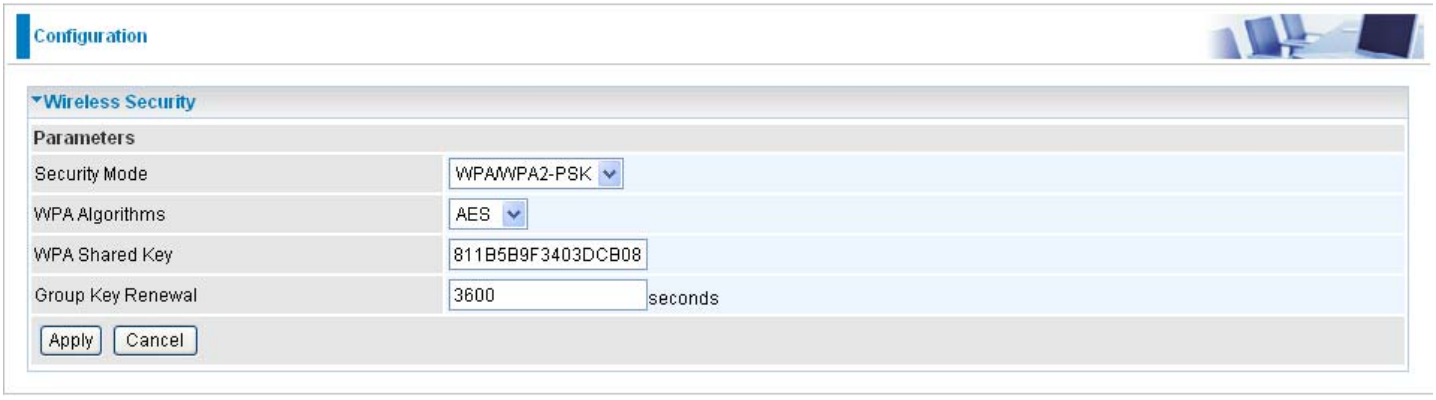


5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.



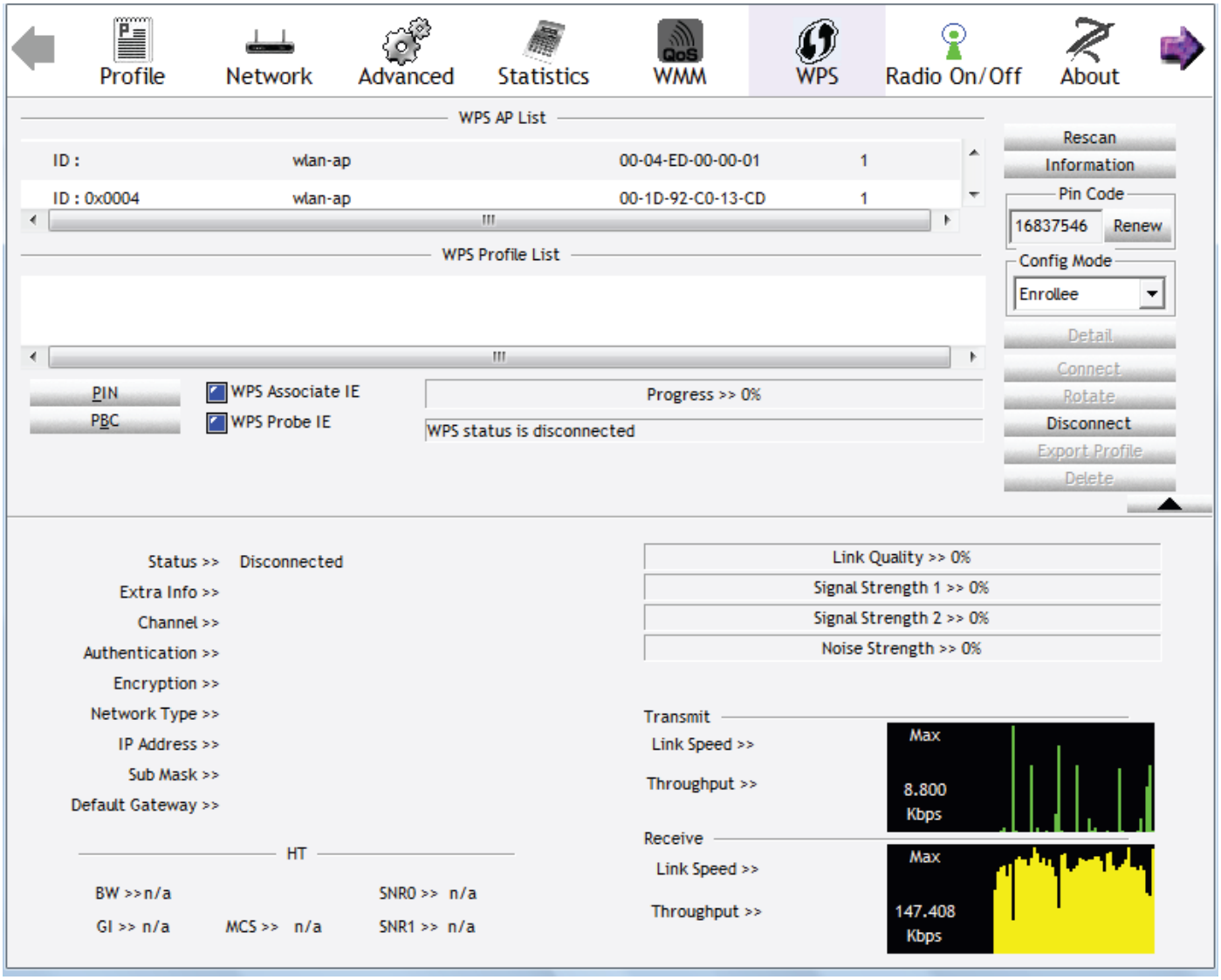
The parameters on both Wireless Configuration and Wireless Security Configuration page are as follows:



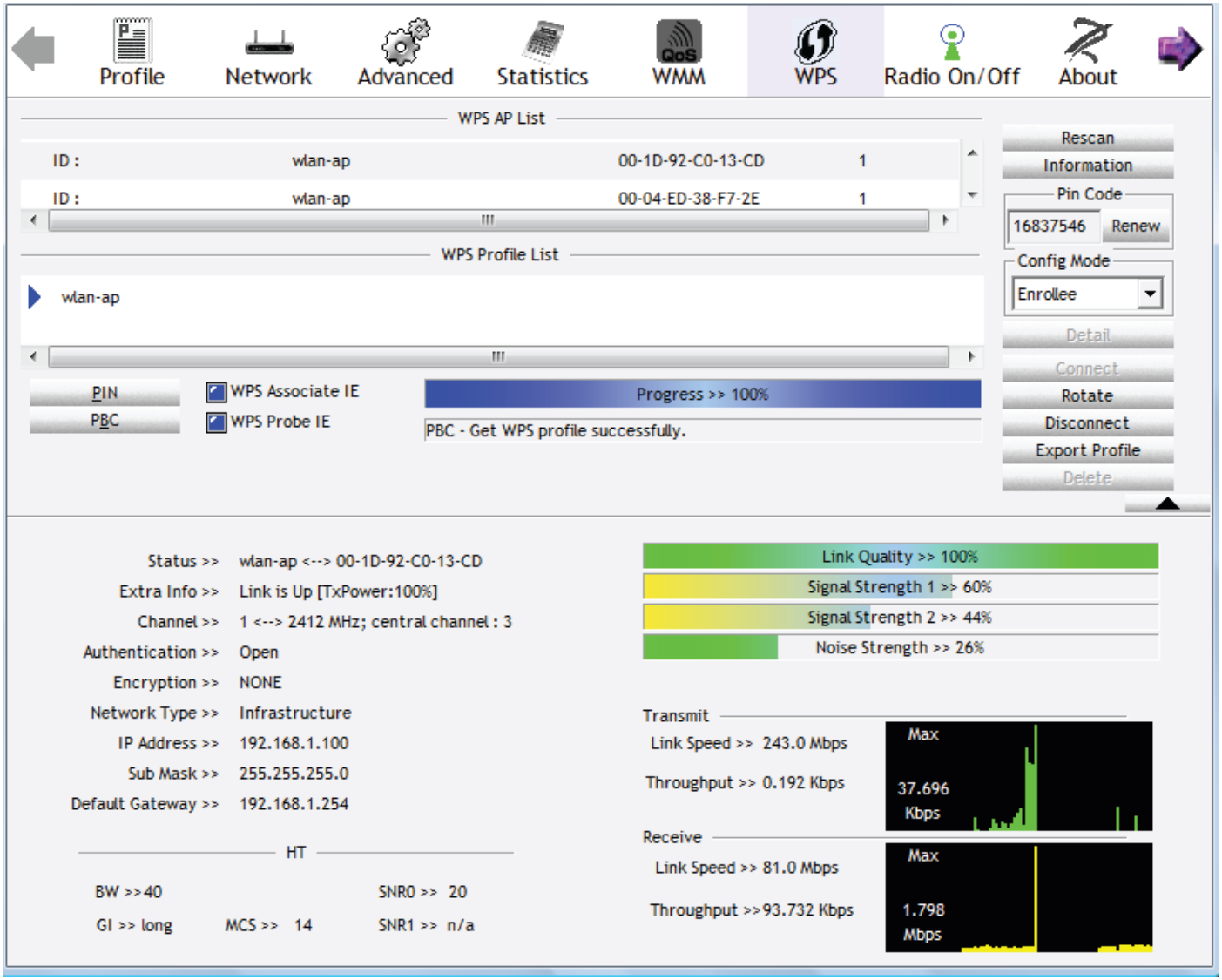


PBC Method:

1. Press the PBC button of the AP.
2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.



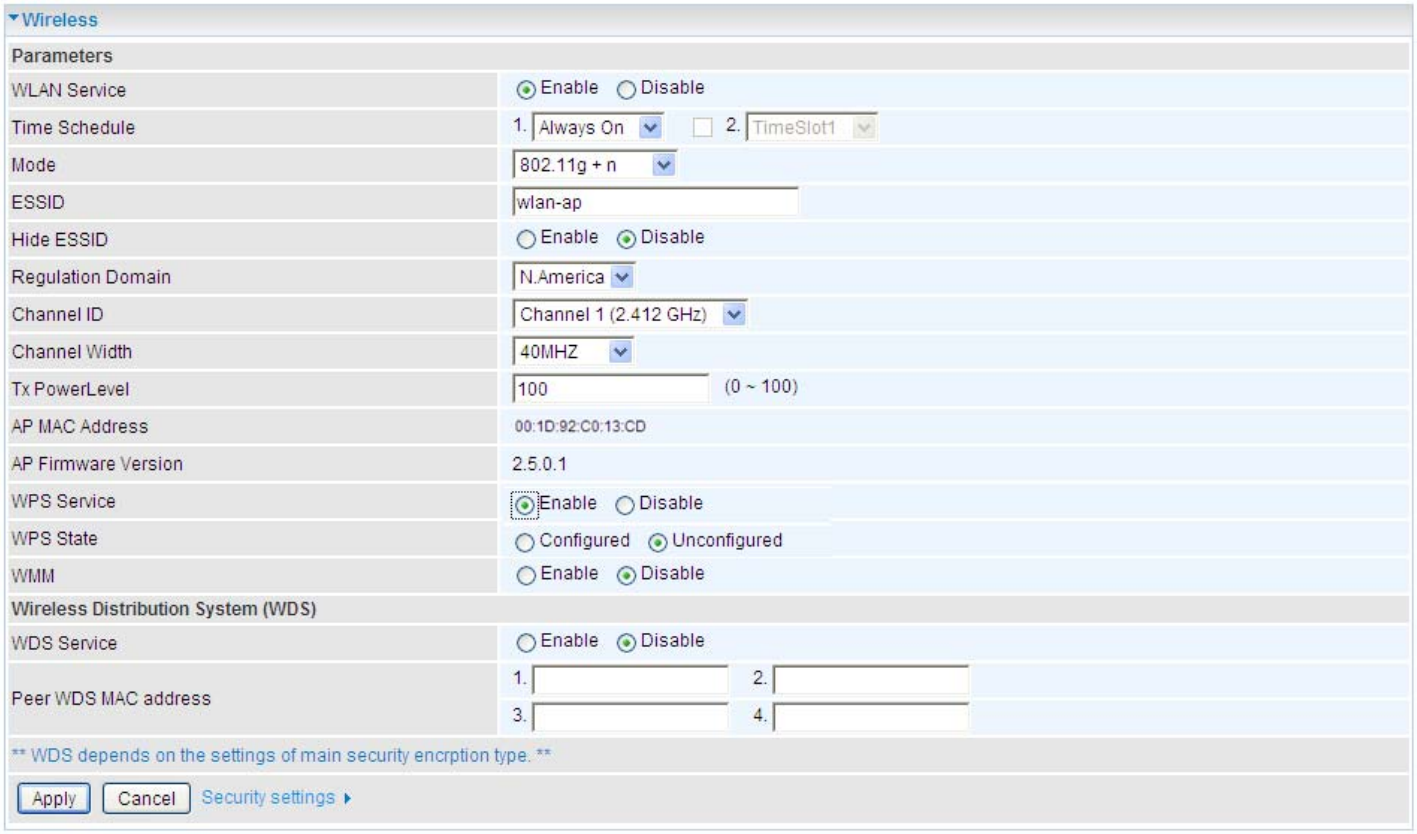
3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



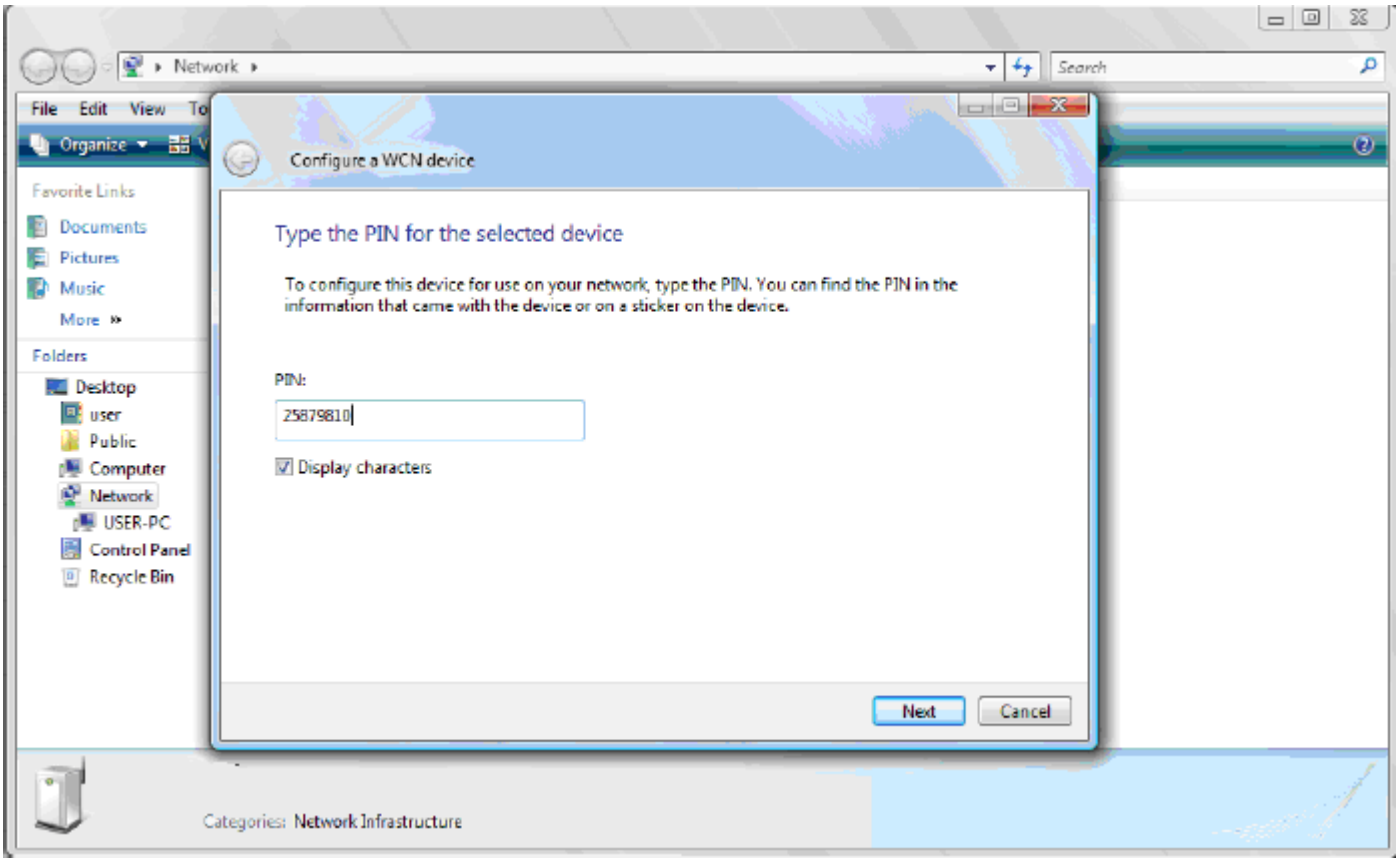
Wi-Fi Network Setup with Windows Vista WCN:

1. Jot down the AP PIN from the Web (eg. 25879810).

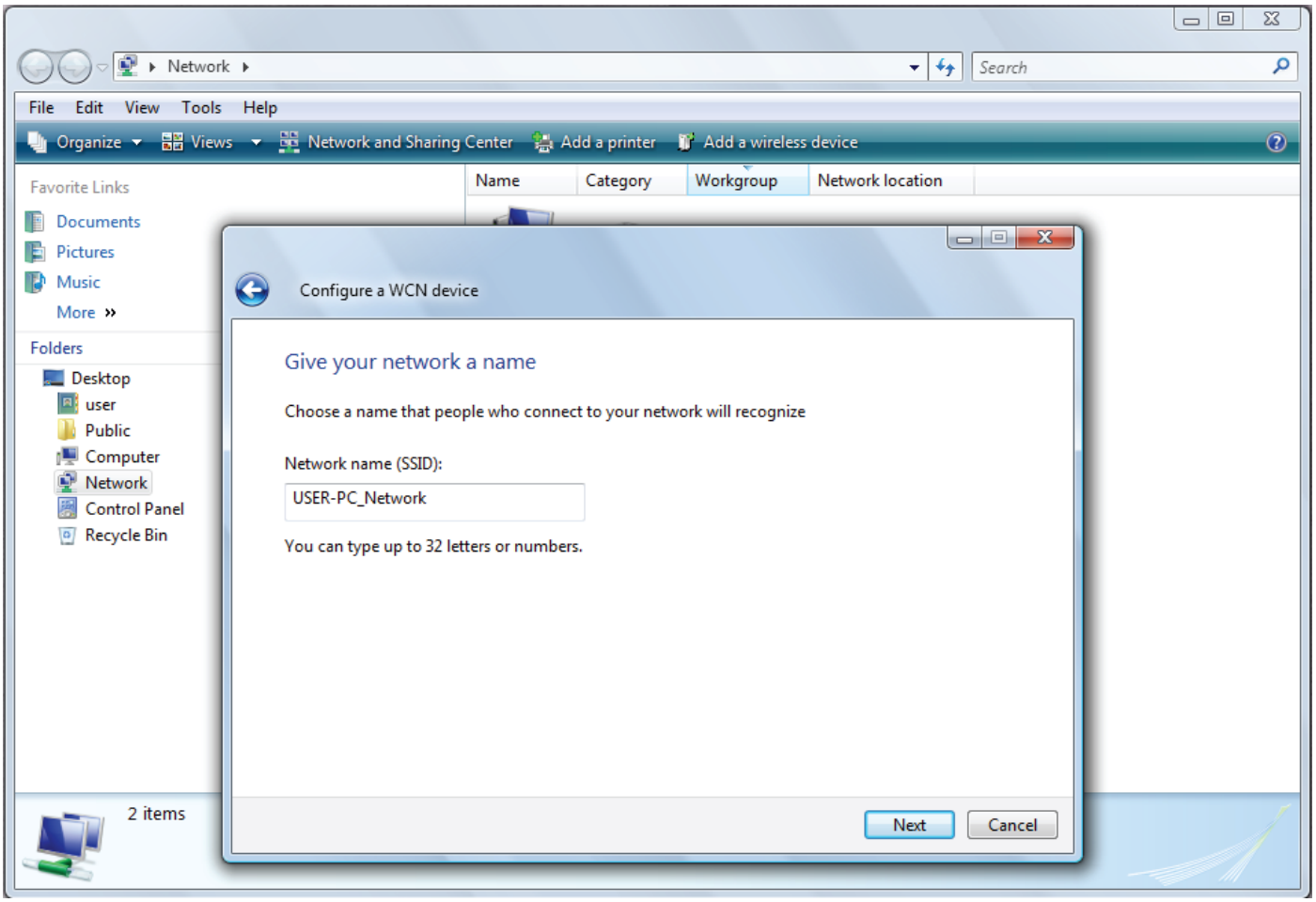
2. Access the Wireless configuration of the web GUI. Enable WPS Service and set the WPS State to Unconfigured then click Apply.



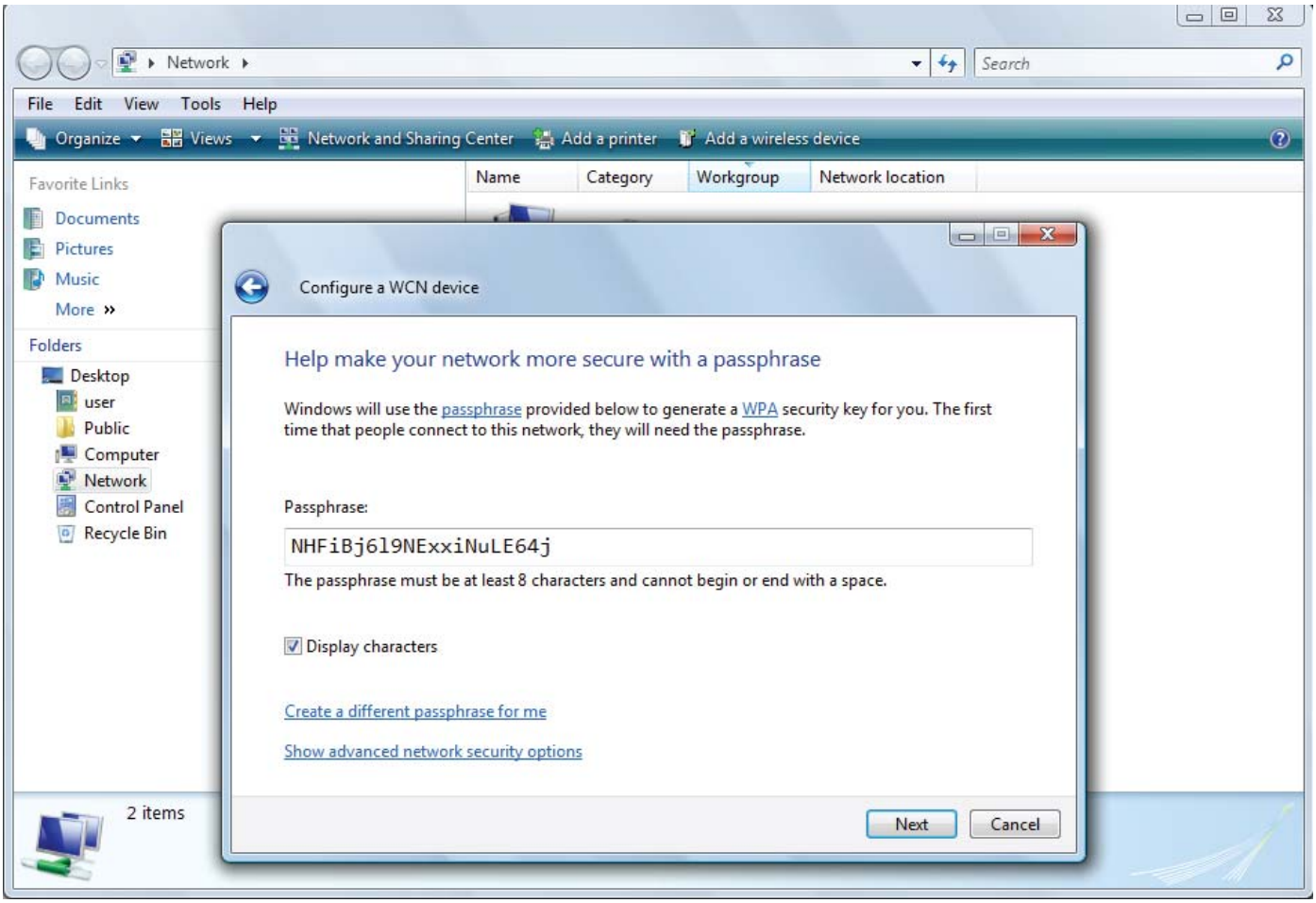
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 7300NX/N *RE* icon and enter the AP PIN in the column provided then press Next.



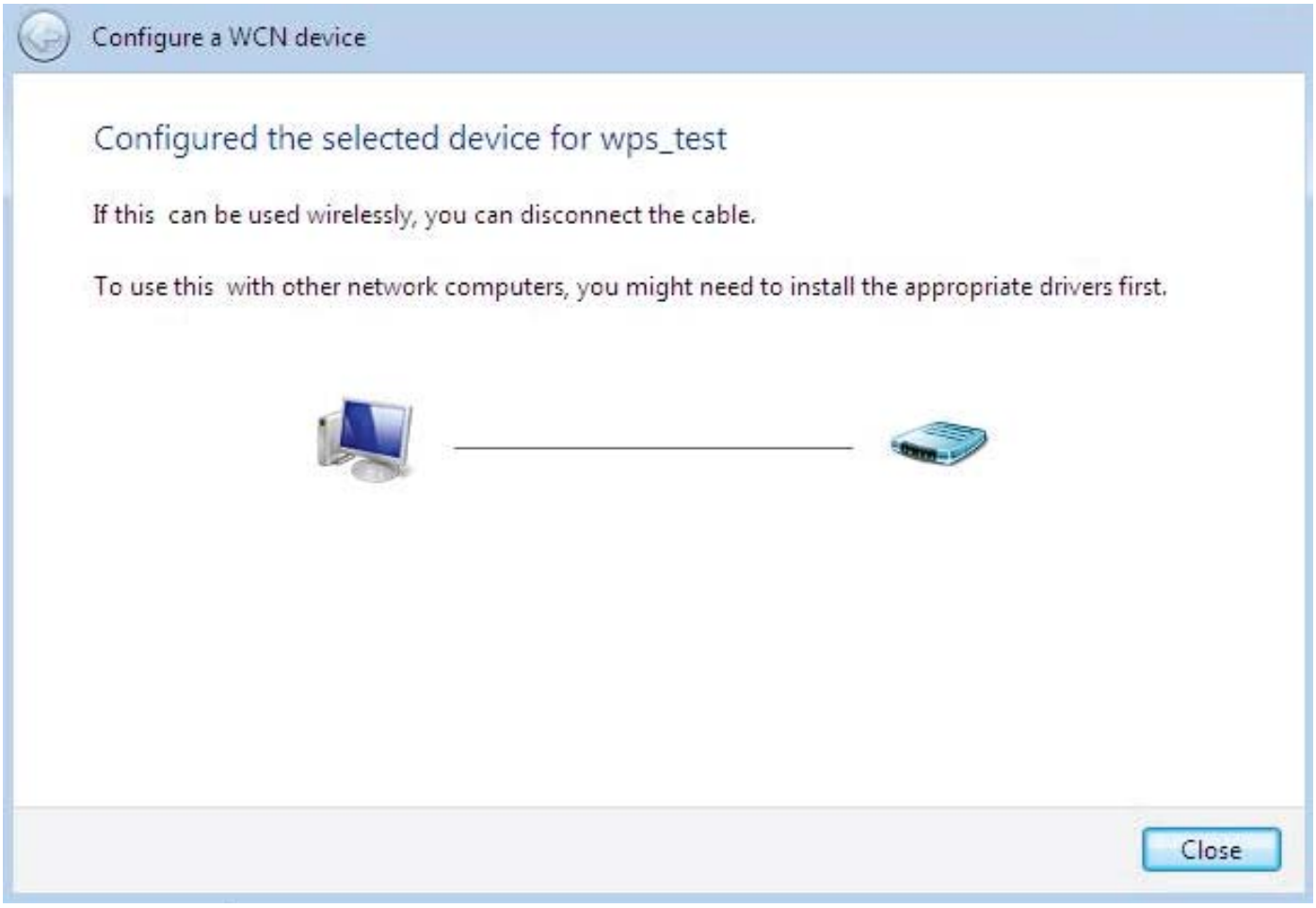
4. Enter the AP SSID then click Next.



5. Enter the Passphrase then click Next.



6. When you have come to this step, you will have completed the Wi-Fi network setup using the built-in WCN feature in Windows Vista.

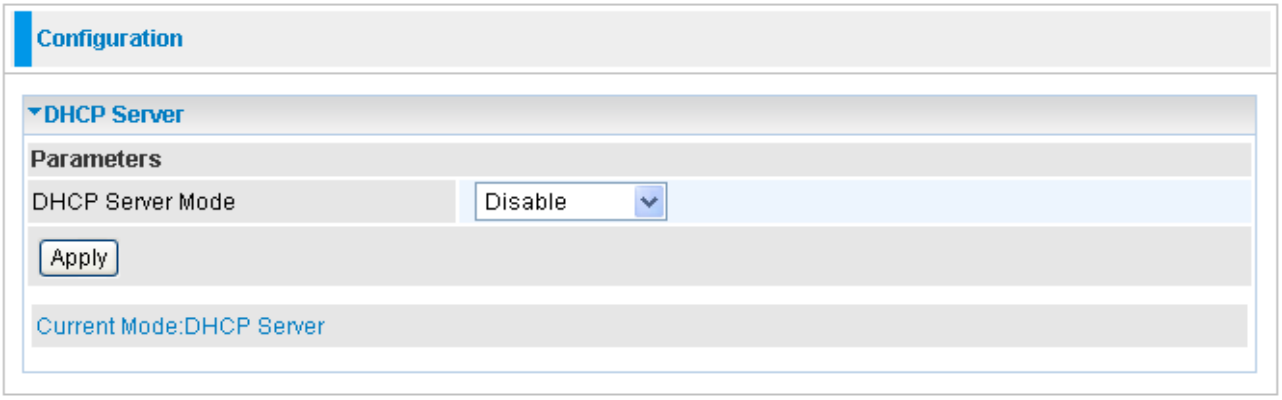

Configure a WCN device
Configured the selected device for wps_test
If this can be used wirelessly, you can disconnect the cable.
To use this with other network computers, you might need to install the appropriate drivers first.
Close

5.3.1.6 DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

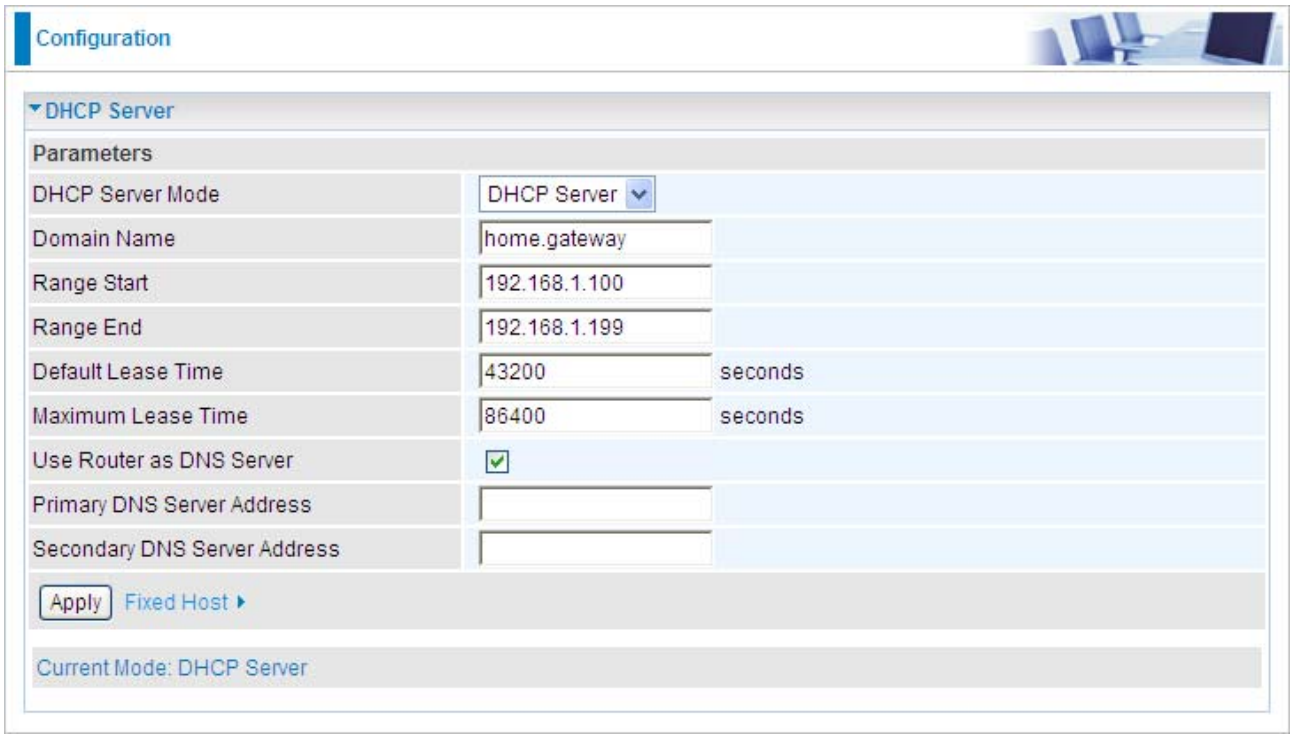
DHCP Server Mode: Disable

To disable the router's DHCP Server, check **Disabled** and then click **Apply.** When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).

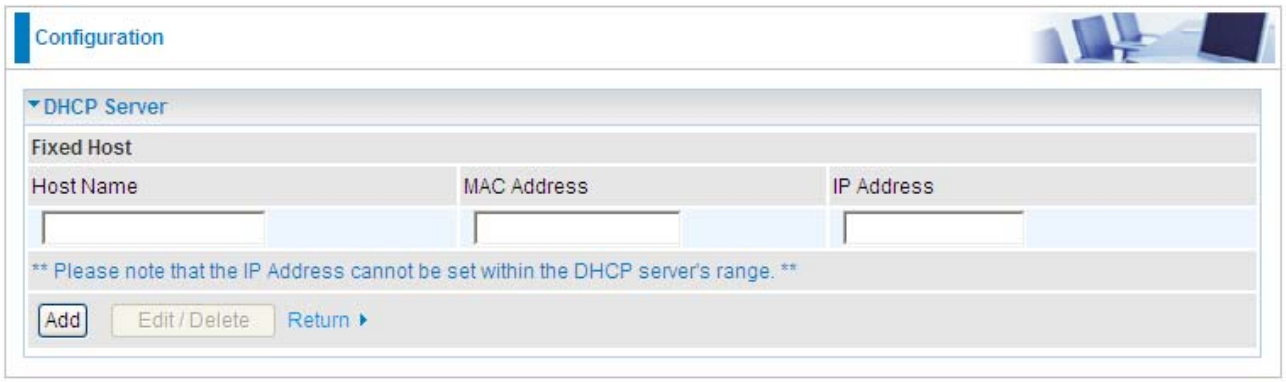


DHCP Server Mode: DHCP Server

To configure the router's DHCP Server, check **DHCP Server**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).



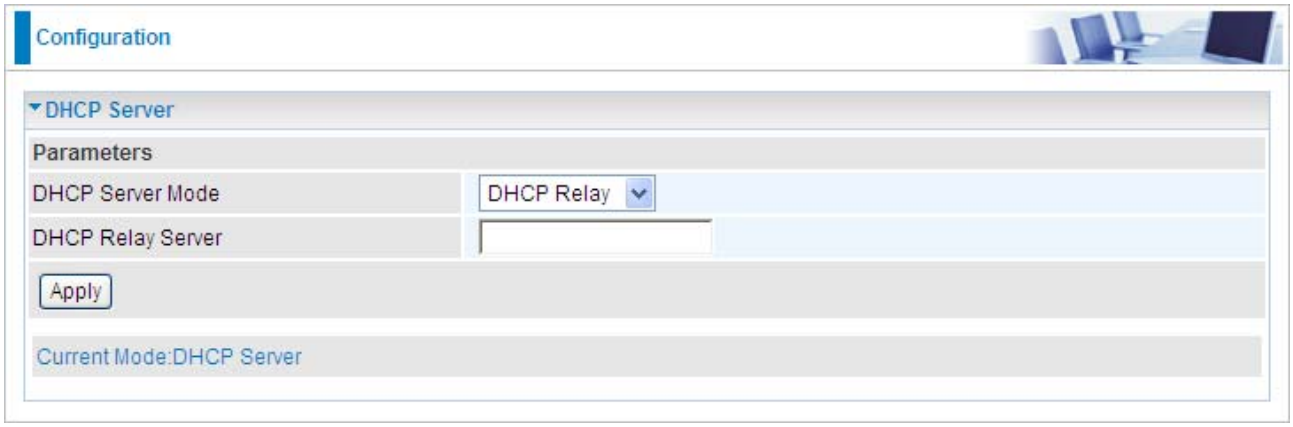
Fixed Host: click Fixed Host link to enter, the following will appear. The Specifyed IP Address will be assigned to the correspongding MAC address by DHCP.



Note: the IP Address you want to enter can't be within the DHCP Server range.
Click Add to add the item, and the corresponding message will be listed below.

DHCP Server Mode: DHCP Relay

If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.



5.3.2 WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are two items within the **WAN** section: **WAN Interface (7300NX only), WAN Profile** and **ADSL Mode.**

5.3.2.1 WAN Interface (BiPAC 7300NX only)

ADSL

WAN Connection

Main Port: Select main port from the drop-down menu. Two connection ports are supported: ADSL and 3G.

Failover Parameters

Failover/Failback: check to determine whether to enable Failover/Failback feature. When enabled, the following parameters will be available.

Backup Port: 3G. Click 3G to enter the 3G configuration page, do the configuration to make it as a backup.

Connectivity Decision: Enter the value for the times when probing failed to switch backup port.

Failover Probe Cycle: Set the time duration for the Failover Probe Cycle to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails.

Failback Probe Cycle: Set the time duration for the Failback Probe Cycle to determine when the router will switch back to the main connection (main port) from the backup connection (backup port) once the main connection communicates again.

Note: The time values entered in Failover Probe Cycle and Failback Probe Cycle fields are set for each probe cycle and decided by Probe Cycle duration multiplied by Connection Decision value (e.g. 60 seconds are multiplied by 12 seconds and 5 consecutive fails).

Detect Rule (either one):

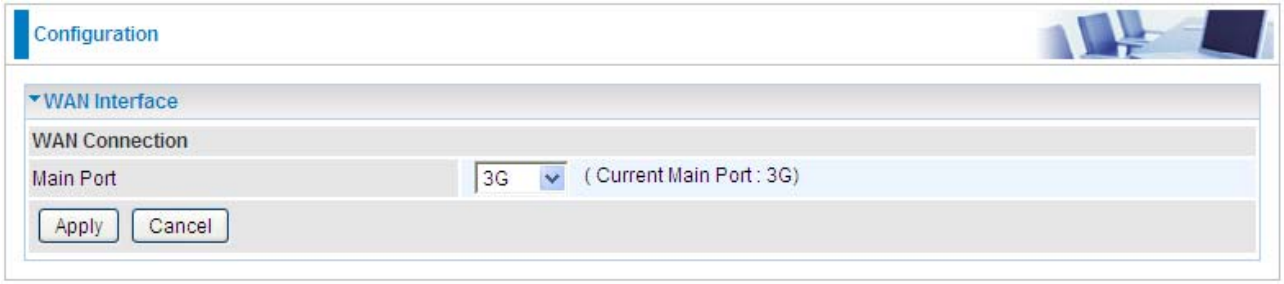
1. ADSL Down

2. Ping Fail

- **No Ping:** It will not send any ping packet to determine the connection. It means to disable the ping fail detection.
- **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every ”Probe Cycle”.
- **Ping Host:** It will send ping packet to specific host and wait response in every “Probe Cycle”. The host must be an IP address.

Click **Apply** to confirm the change.

3G



Main Port: Select the main port from the drop-down menu.

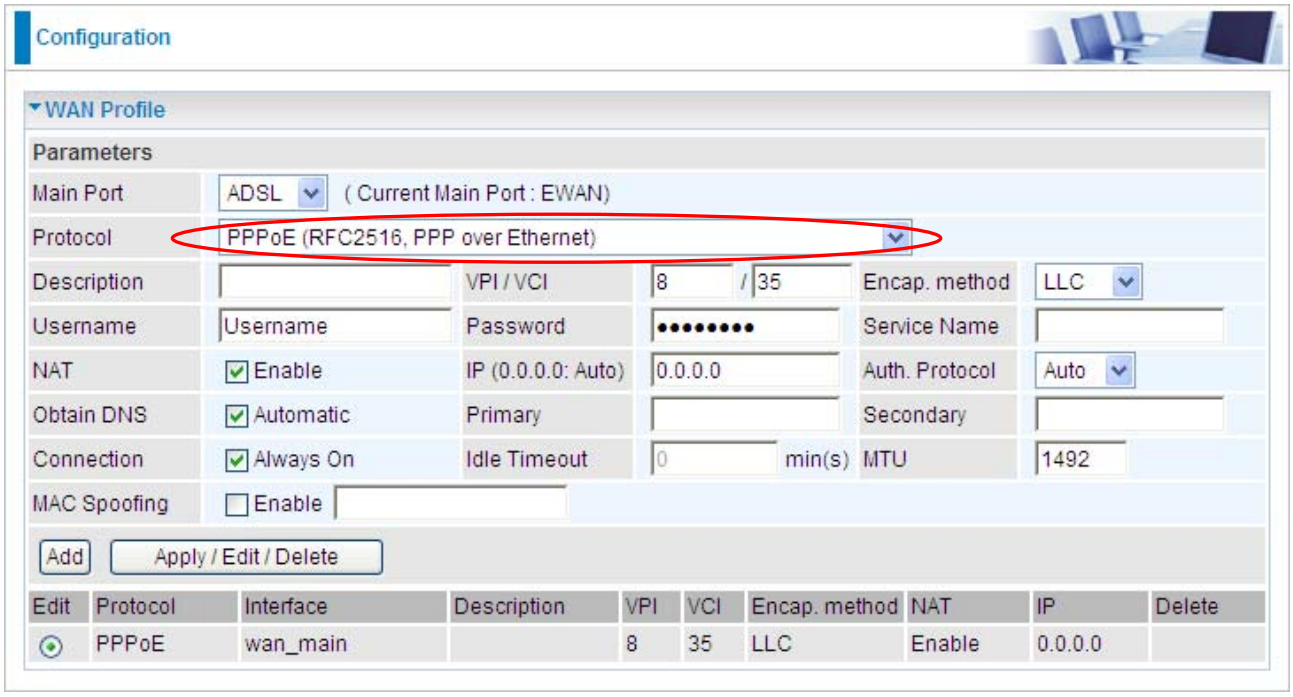
Click **Apply** to confirm the change.

5.3.2.2 WAN Profile

Main Port--ADSL

PPPoE Connection (ADSL)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



Description: A user-definable name for this connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format, the default is LLC. Select the one provided by your ISP

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Connection:

⊙ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

⊙ **Connect to Demand (un-select Always On):** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.

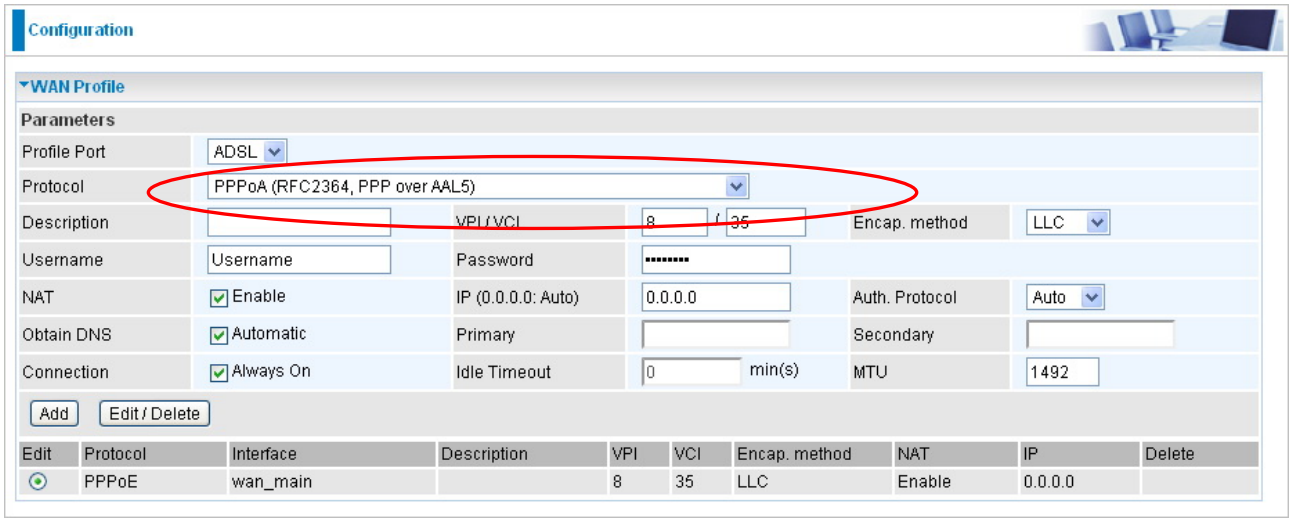
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

PPPoA Connection (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.



Description: User-definable name for the connection.

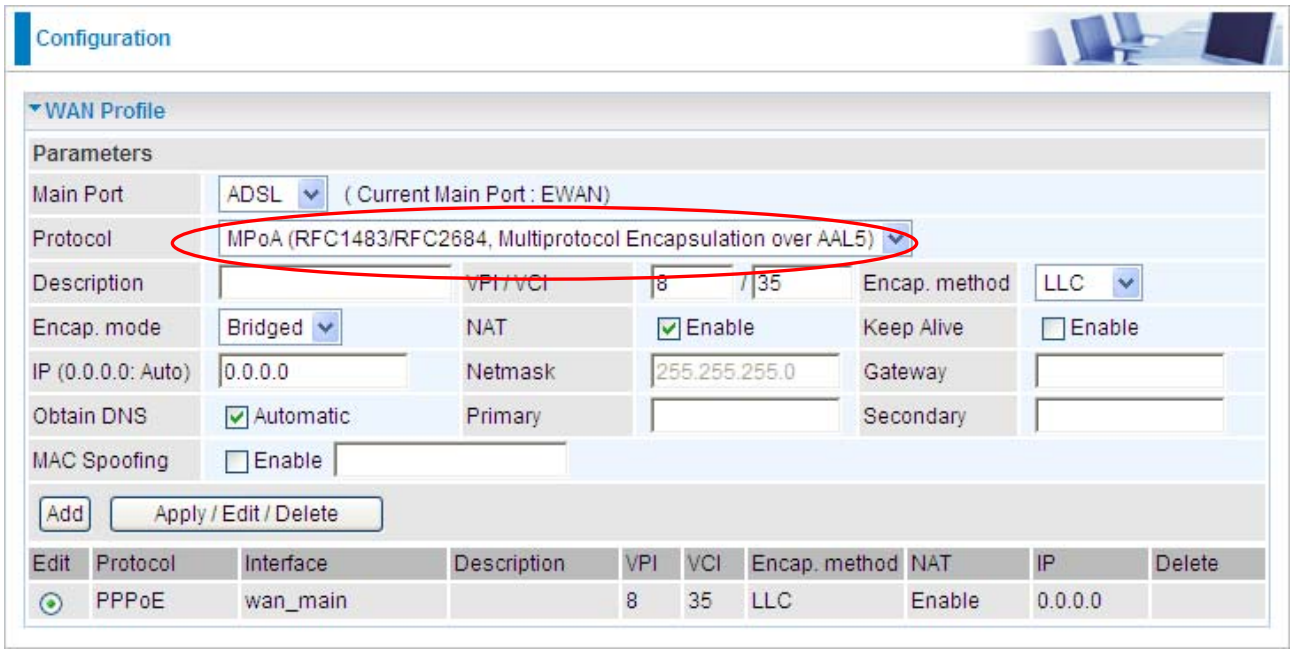
VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format, the default is LLC. Select the

one provided by your ISP

- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Authentication Protocol:** Default is **Auto**. Your ISP should advise you on whether to use **Chap** or **Pap.**
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.
- **Connection:**
  - ⊙ **Always on:** The router will establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
  - ⊙ **Connect to Demand (un-select Always On):** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.
- **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that the IP attempts to send through the interface.

MPoA Connection (ADSL)



Description: Your description of this connection.

VPI and VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format, the default is LLC. Select the one provided by your ISP.

Encap. mode: Choose whether you want the device to function as bridge mode or routing mode.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Keep Alive: Set Enable to keep the router on line and prevent to be disconnected by the ISP when they think there is no activity on the line.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Netmask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

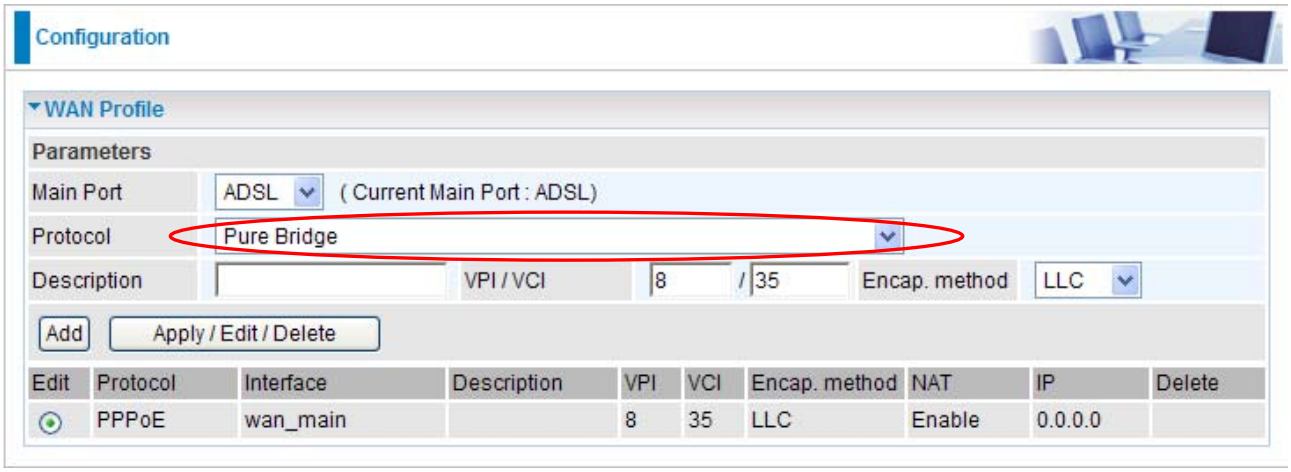
Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

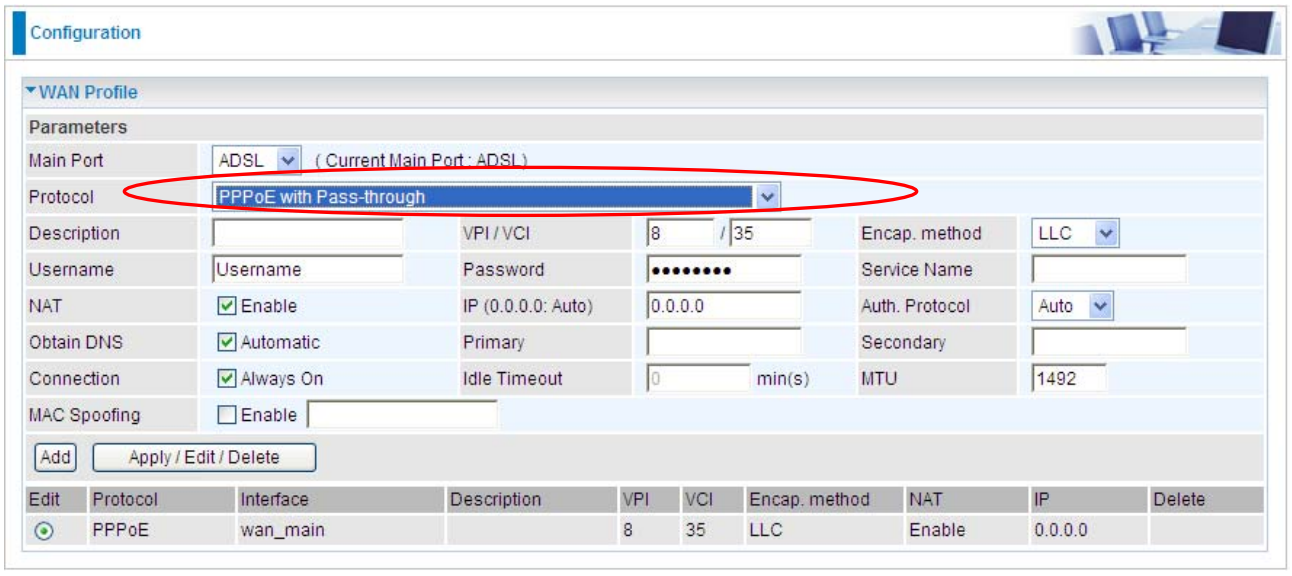
MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Pure Bridge Connections (ADSL)



- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, this is provided by your ISP.

PPPoE with Pass-through (ADSL)



- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP.
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128**

alphanumeric characters (case sensitive)

- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Auth. Protocol:** Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
- **Connection:**

  ⊙ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

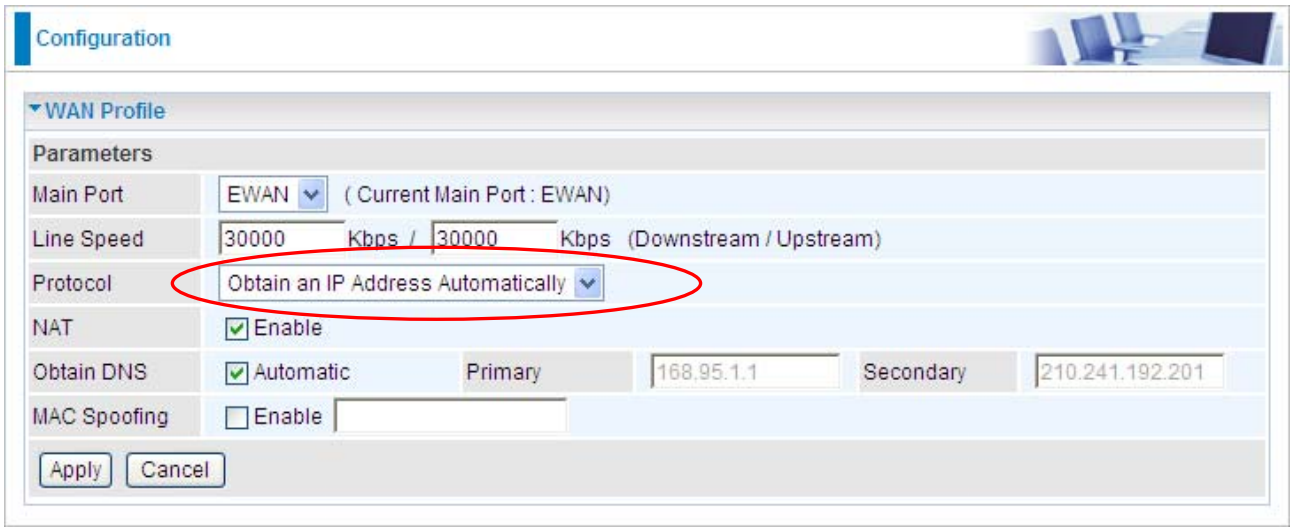
  ⊙ **Connect to Demand (un-select Always On):** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.
- **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.
- **MAC Spoofing:** This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Main Port—EWAN (BiPAC 7300N *RE* only)

Besides using ADSL to get connected to the Internet, BiPAC 7300N *RE* offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems, VDSL and fibre optic lines. This alternative, yet faster method to connect to the internet will provide users with more flexibility to get online

Obtain an IP Address Automatically (EWAN)

When connecting to the ISP, BiPAC 7300N *RE* also functions as a DHCP client. BiPAC 7300N RE can automatically obtain an IP address, netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

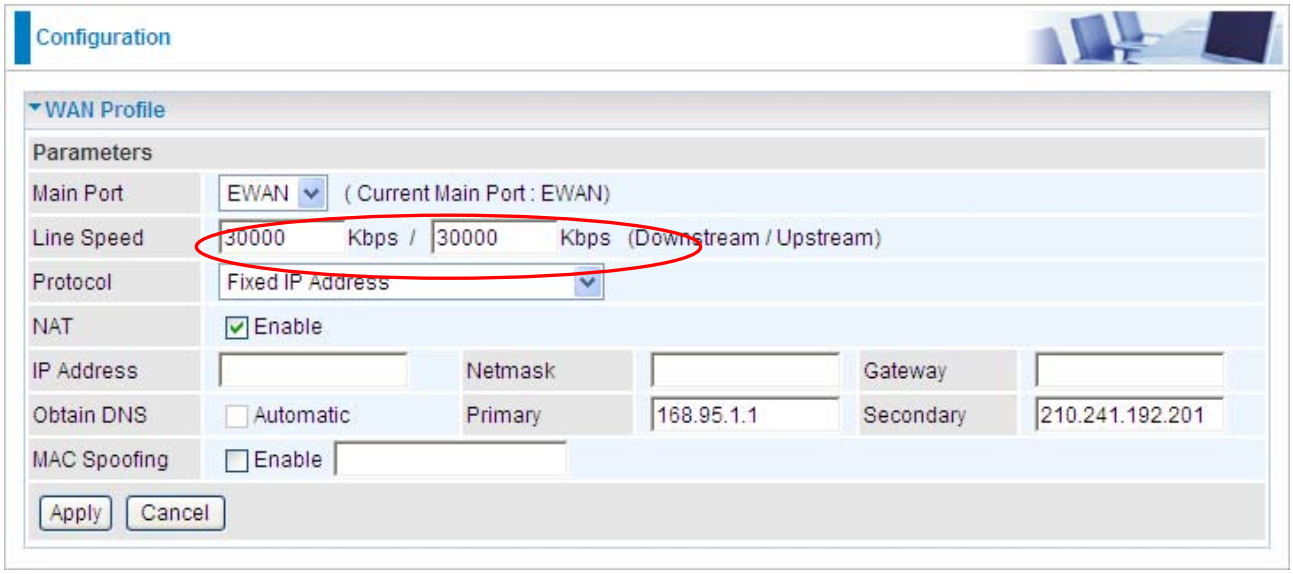
Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Fixed IP Address (EWAN)

Select this option to set static IP information. You will need to enter in the Connection type, IP address, netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Enter your WAN IP address.

IP Netmask: Type the netmask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP)

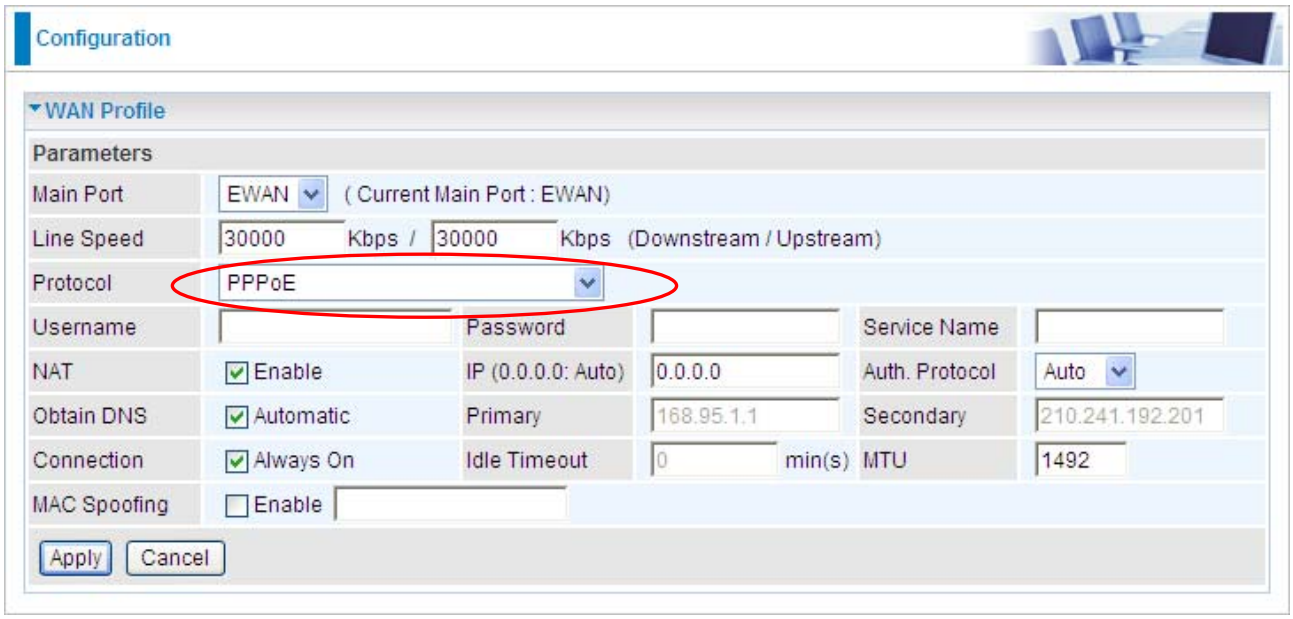
Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

PPPoE (EWAN)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: Enter a name for this connection.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

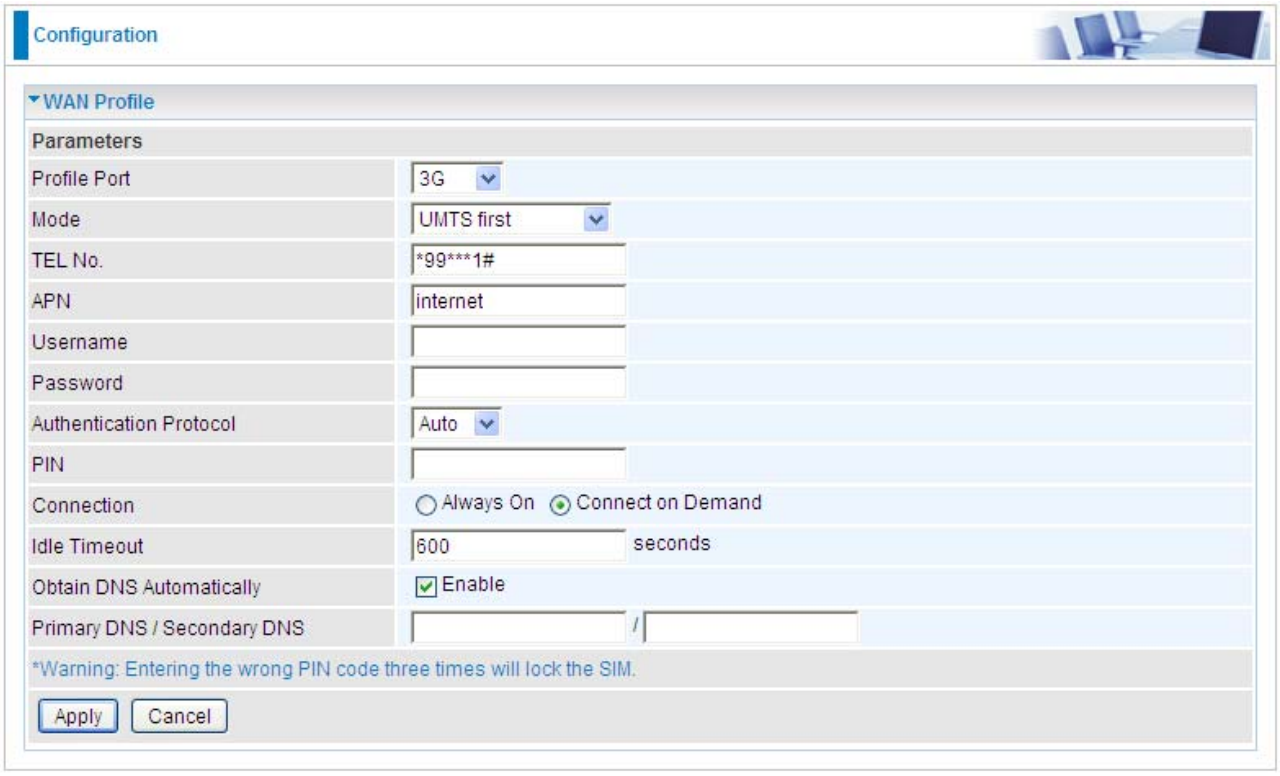
Auth. Protocol: Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router’s MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Main Port—3G (BiPAC 7300NX only)



Mode: There are 5 options of phone service standards: GSM only, UTMS only, GPRS/EDGE first, UMTS first, and Automatic. If you are uncertain what services are available to you, then please select Automatic.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may provide by your mobile service provider.

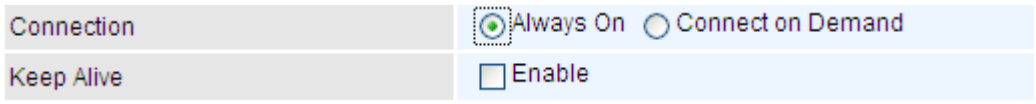
APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP or CHAP.

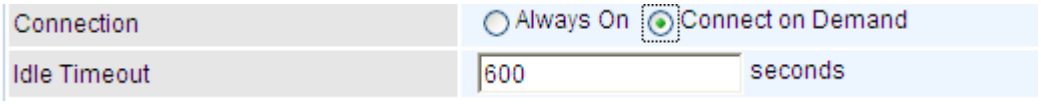
PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

Connection:



Always On: Check Enable to allow the router automatically reconnects the connection when ISP disconnects it.

Keep Alive: Check Enable to allow the router to send message out every 30sec to prevent the connection being dropped by ISP.



Connection on Demand: If you want to establish a 3G session only when there is a packet requesting access to the Internet. In this mode, you must set Idle Timeout value at same time.

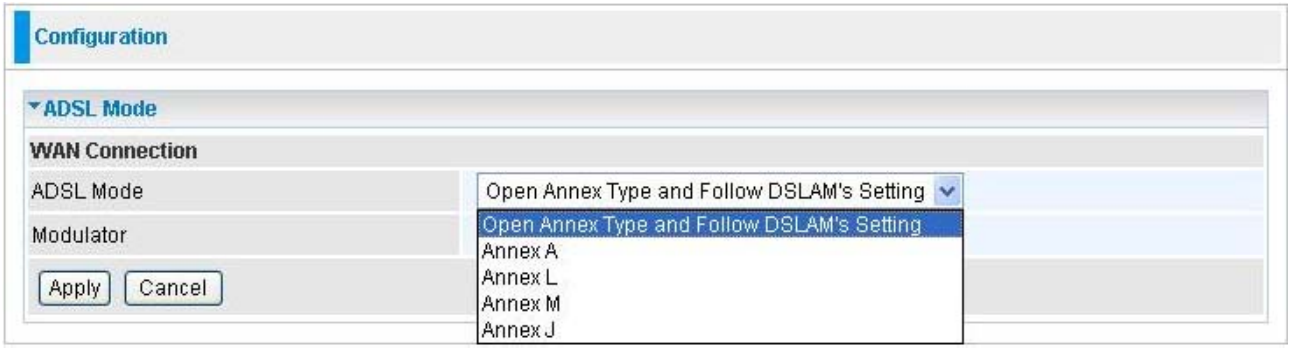
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The idle timeout value is not allowed to be set under 10 seconds. Default is 600 seconds.

Obtain DNS Automatically: Select this check box to activate DNS automatically.

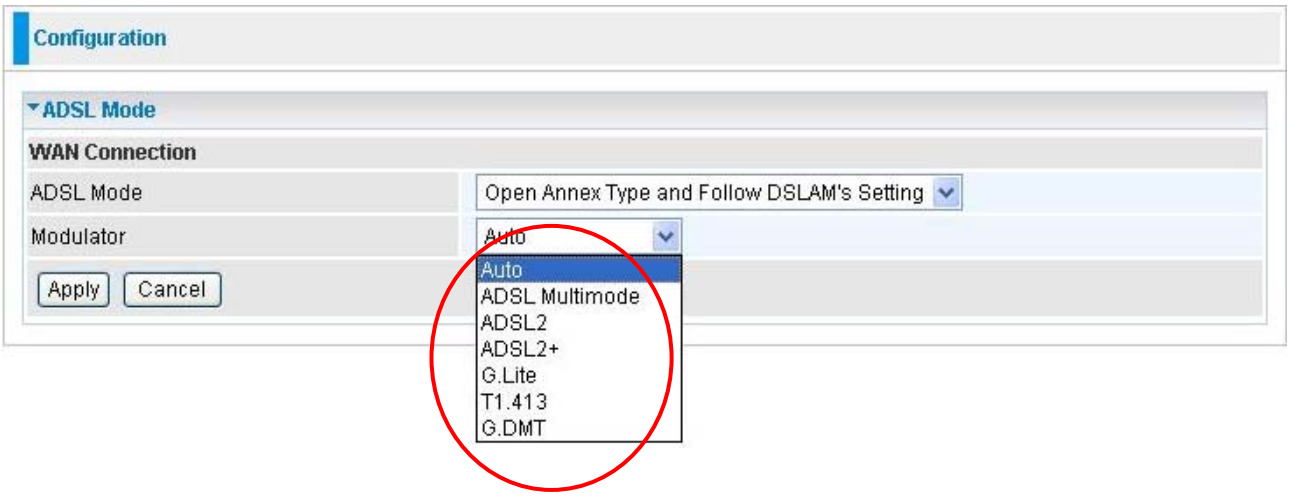
Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Note: If you don't know how to set these parameters, please keep them untouched.

5.3.2.3 ADSL Mode

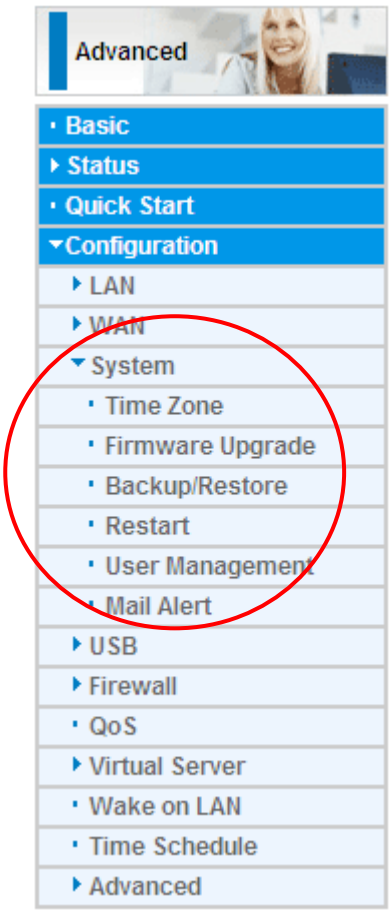


- **ADSL Mode:** There are four modes "**Open Annex Type and Follow DSLAM's Setting**", "**Annex A**", "**Annex L**", "**Annex M**" and **"Annex J"** that user can select for this connection.
- **Modulator:** There are seven modes "**AUTO**","**ADSL multimode**","**ADSL2**","**ADSL2+**", **"G.Lite:**", **"T1.413"** and **"G.DMT"** that user can select for this connection.



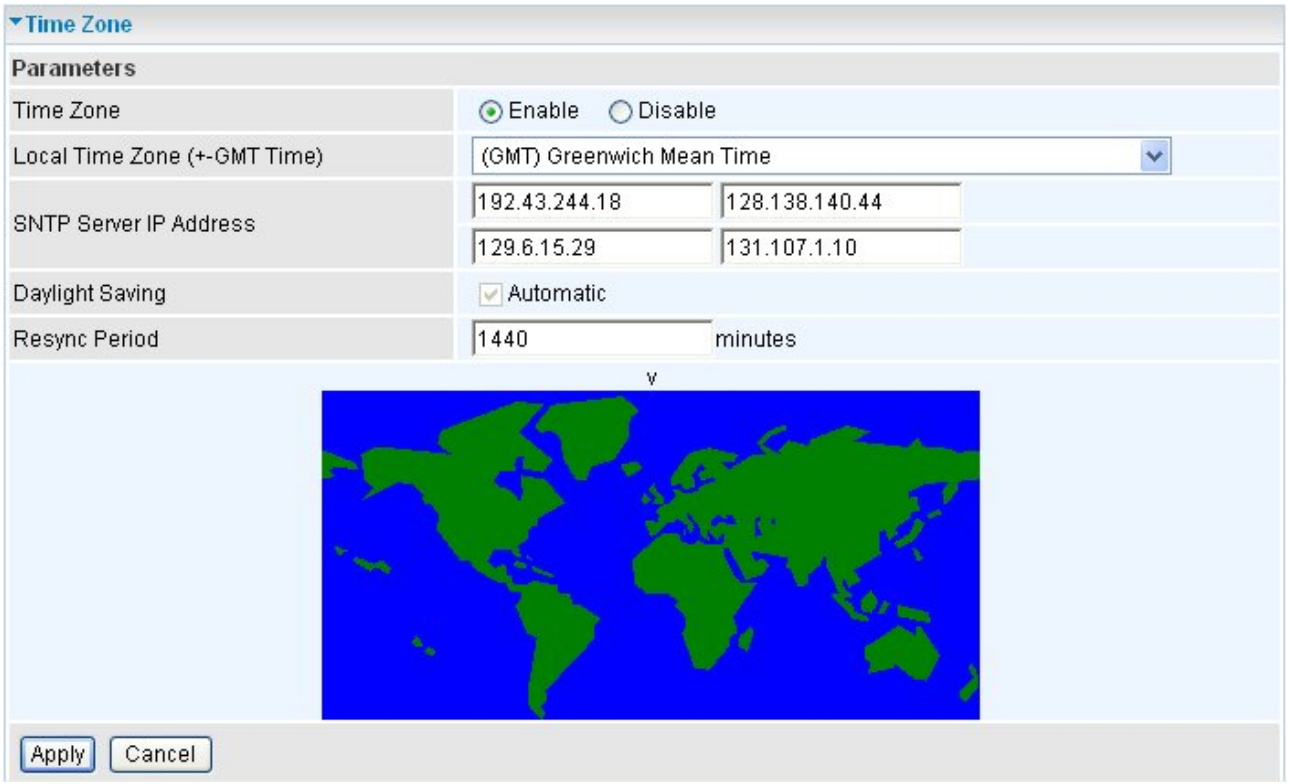
5.3.3 System

There are five items within the **System** section: **Time Zone, Firmware Upgrade, Backup/Restore, Restart**, **User Management** and **Mail Alert.**



(BiPAC 7300NX)

5.3.3.1 Time Zone



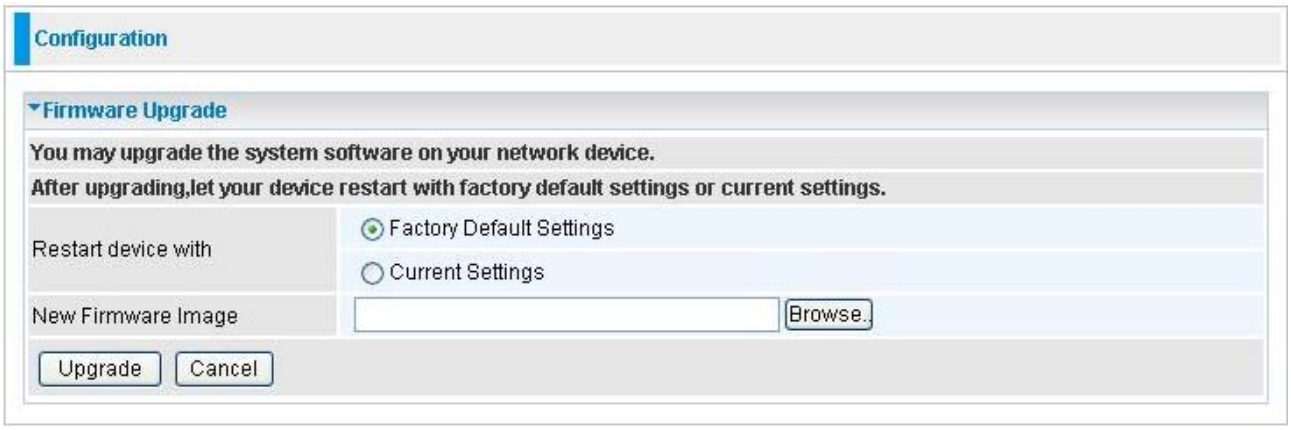
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

5.3.3.2 Firmware Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

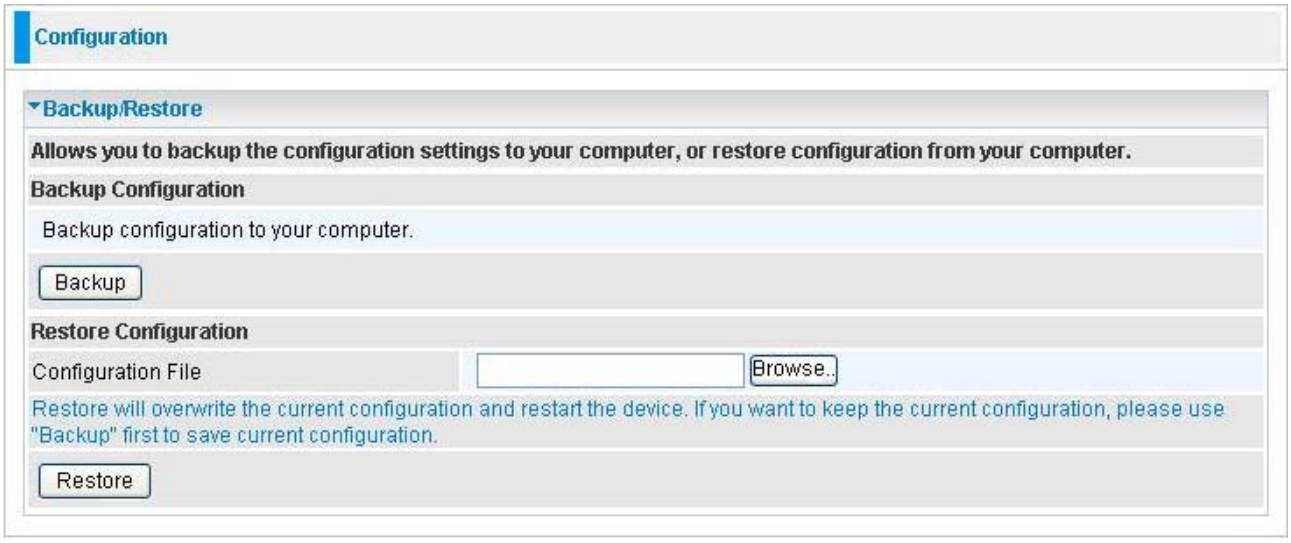


- **Restart Device with:** To choose "Factory Default Settings" or "Current Settings" which uses your current setting on the new firmware (it is highly advised to use Factory Default Settings over Current Settings for a clean firmware upgrade).
- **New Firmware Image:** Type in the location of the file you wish to upload in this field or click **Browse…** to locate it.
- **Browse…:** Click **Browse…** to find the file with the **.afw** file extension that you wish to upload. Remember that you must decompress compressed (.zip) files before you can upgrade from the file.
- **Upgrade:** Click **upgrade** to begin the upload process. This process may take up to three minutes.

Warning

DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. Please see section 2.4 for emergency recovery procedures.

5.3.3.3 Backup / Restore


Configuration
Backup/Restore
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse..
Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

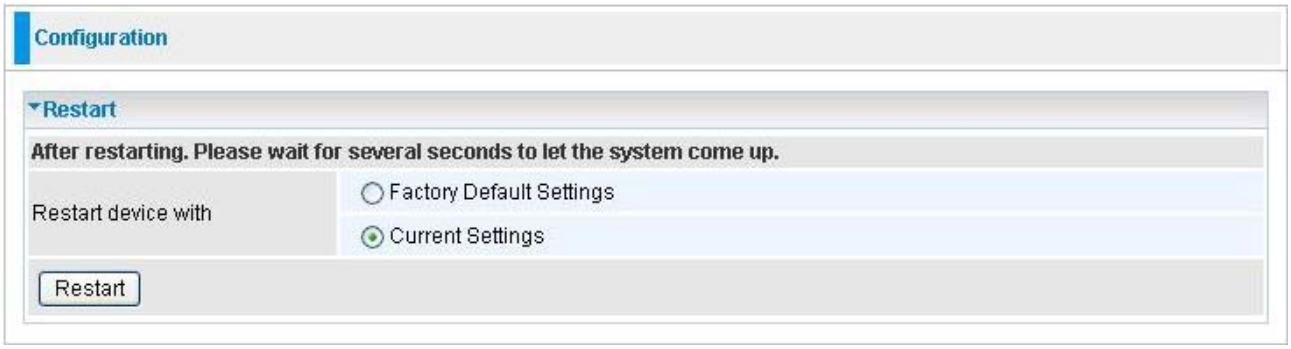
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse…** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

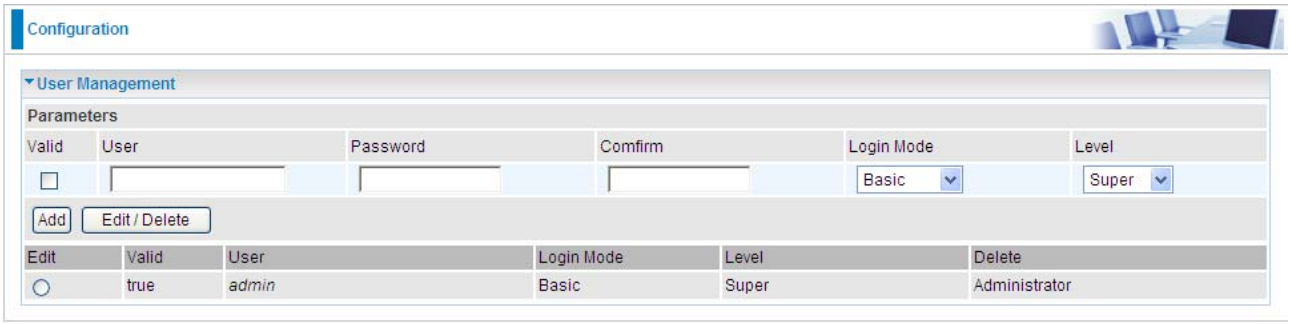
5.3.3.4 Restart Router

Click **Restart** with option **Current Settings** to reboot your router and save the current configuration to device.



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

5.3.3.5 User Management



In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked **Edit** on the account you want to edit**,** the information of the account will be displayed above. Just go ahead and change the password. You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under **Delete** and then press the **Edit/Delete** button.

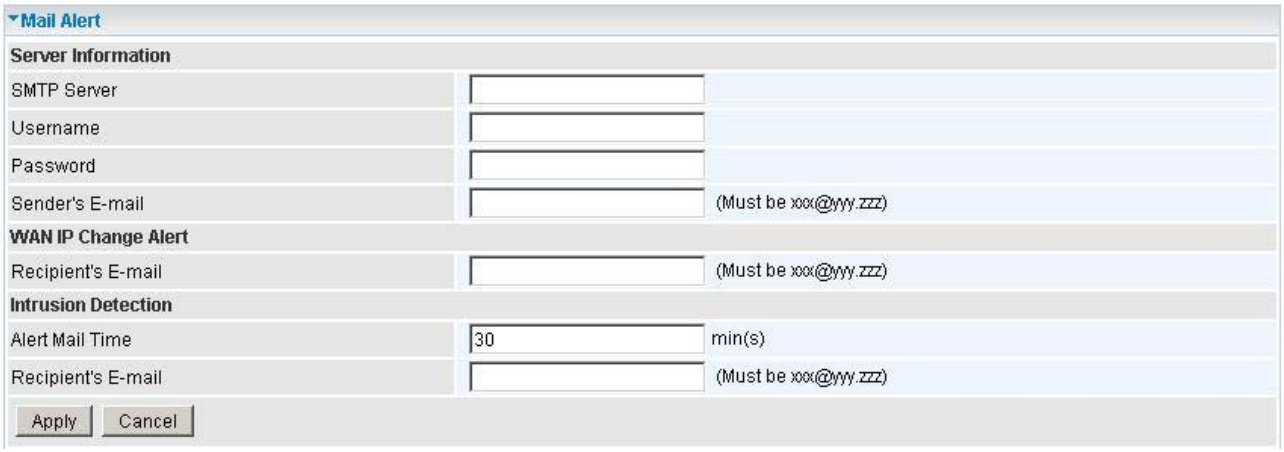
You are strongly advised to change the password on the default "**admin**" account when you

receive your router, and any time you reset your configuration to Factory Defaults.

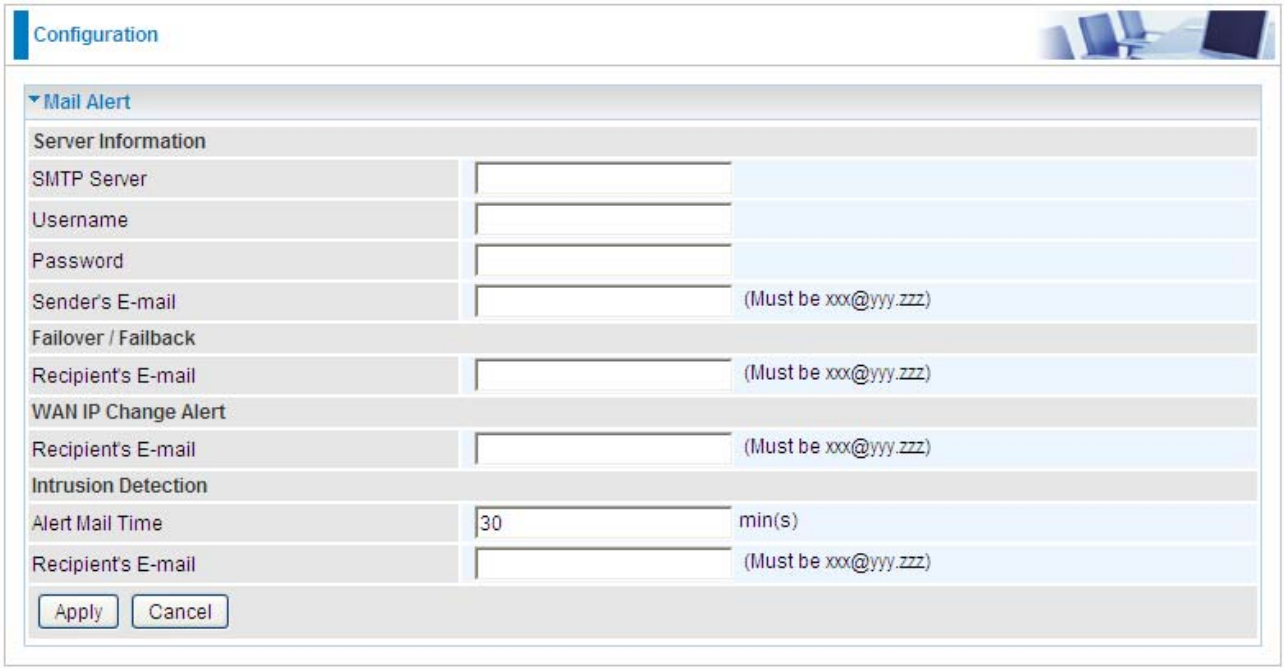
5.3.3.6 Mail Alert

Send a log via email, if WAN IP is changed or if intruders accessing your computer without permission.

BiPAC 7300N *RE*



- **SMTP Server:** Enter the SMTP server that you would like to use for sending emails.
- **Username:** Enter the username of your email account to be used by the SMTP server.
- **Password:** Enter the password of your email account.
- **Sender's Email:** Enter your email address.
- **Recipient's Email (WAN IP Change Alert):** Enter the email address that will receive the alert message once an WAN IP change has been detected.
- **Alert Mail Time (Intrusion Detection):** The interval for sending alert mail.
- **Recipient's Email (Intrusion Detection):** Enter the email address that will receive the alert message once intrusion has been detected.



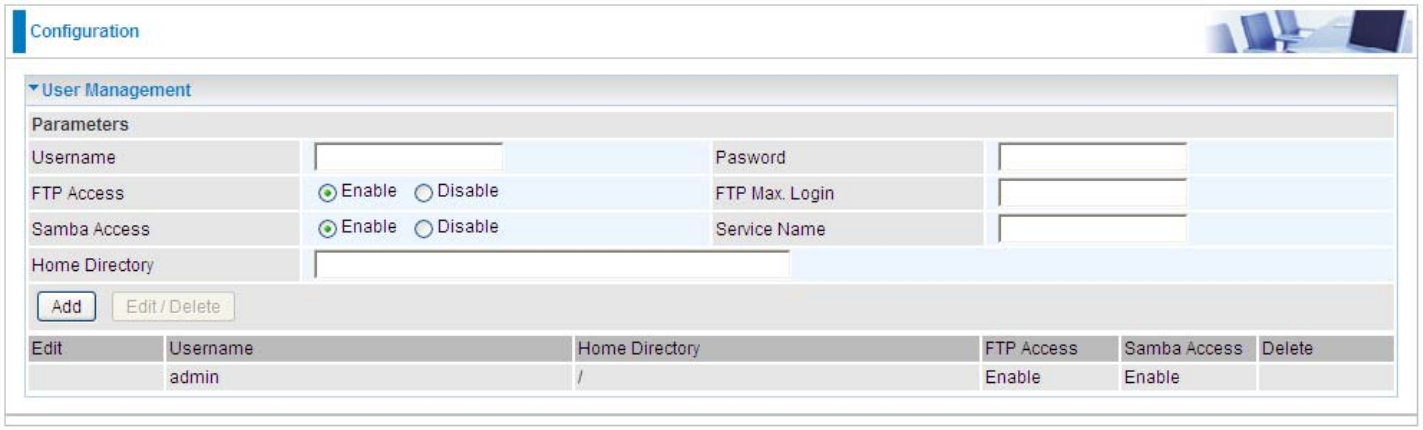
- **SMTP Server:** Enter the SMTP server that you would like to use for sending emails.
- **Username:** Enter the username of your email account to be used by the SMTP server.
- **Password:** Enter the password of your email account.
- **Sender's Email:** Enter your email address.
- **Recipient's E-Mail:** Enter the email address that will receive the alert message when Failover/failback incident happens.
- **Recipient's Email (WAN IP Change Alert):** Enter the email address that will receive the alert message once an WAN IP change has been detected.
- **Alert Mail Time (Intrusion Detection):** The interval for sending alert mail.
- **Recipient's Email (Intrusion Detection):** Enter the email address that will receive the alert message once intrusion has been detected.

5.3.4 USB

Besides connecting to 3G modem, USB 2.0 port can also provide storage features, and server as FTP Server and Samba Server. USB Server has integrated FTP Server feature. Through FTP Server, Samba Server user can management the account, set the authority of download and upload.

There are five items within the USB section: **User Management, Storage, Samba Server, FTP**.

5.3.4.1 User Management



Username: Enter the name for the account.
Password: Set the password for the account.

FTP Access: If you enable this function, this account has the access authority to FTP Server.
Max. Login: This option specifies the maximum number of users (both anonymous and non-anonymous) that are allowed to be using the FTP server simultaneously.

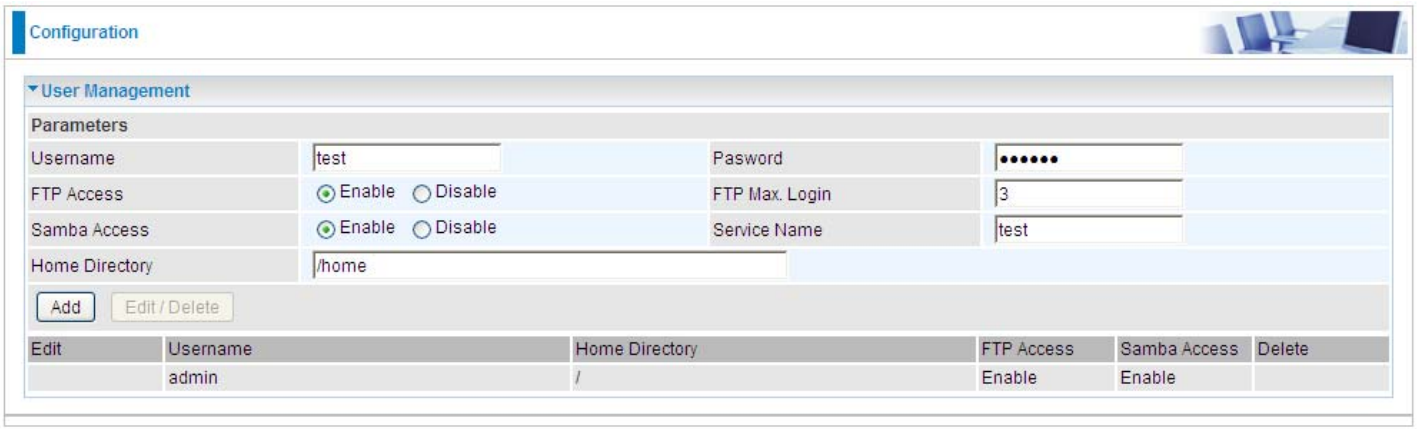
Samba Access: If you enable this function, this account has the access authority to Samba Server.
Service Name: enter the name for this Samba service.

Home Directory: the home directory for the account. If you type '/', the account will see all the folders in the USB device, which means the whole is your work folder. If you type "/home", your work folder is home, and the folders within home will be shown to you.

Add: Click this button to add a new account and it will appear at the bottom table.
Edit/Delete: Choose one account which you wish to Edit/Delete, and then click "Edit/Delete".

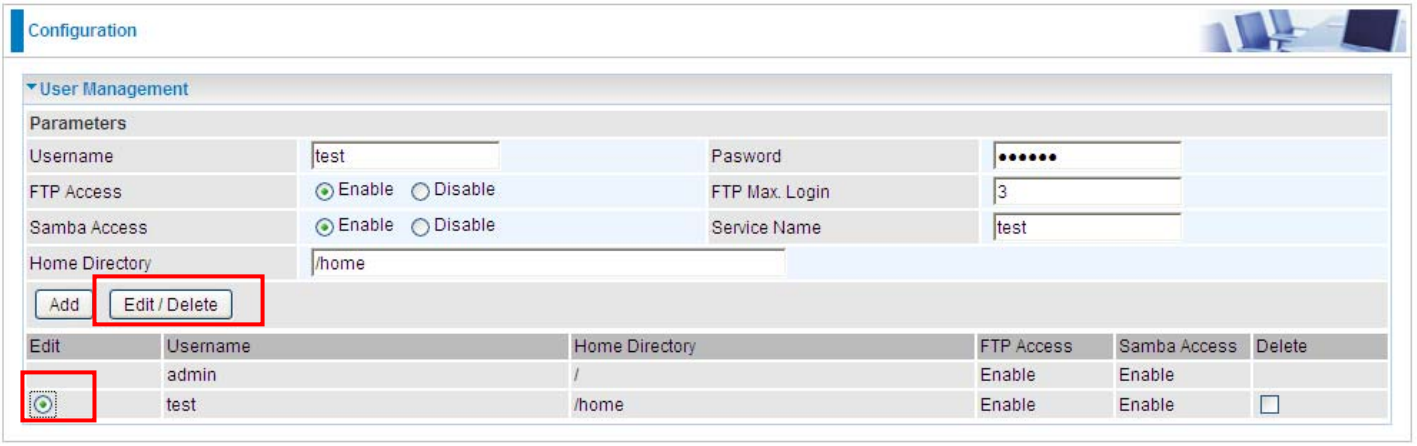
Add/Delete User

1. Enter username and password (admin is the default user)

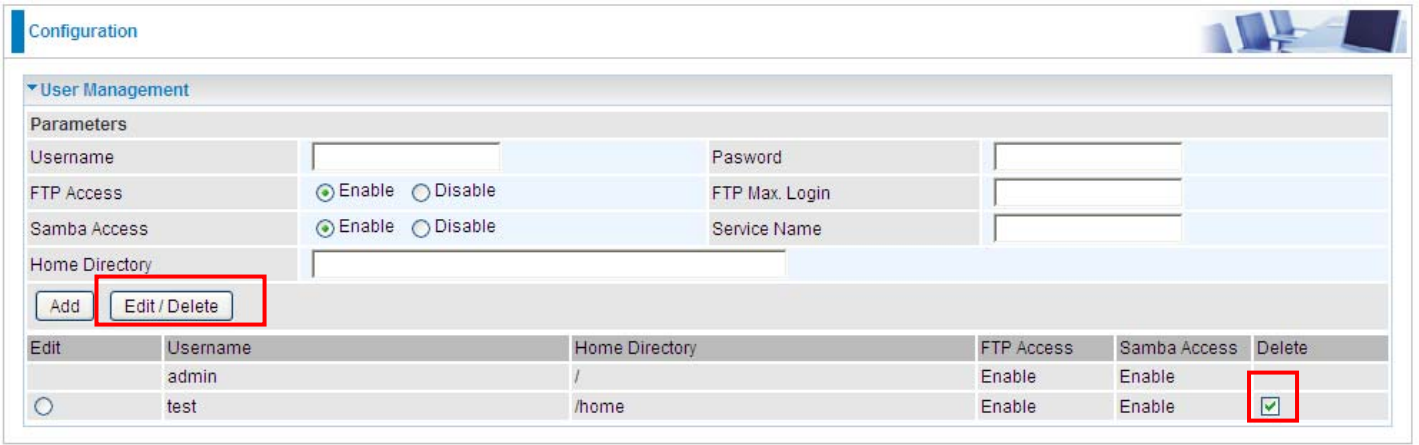


2. Click **Add**. The new user account will display below.

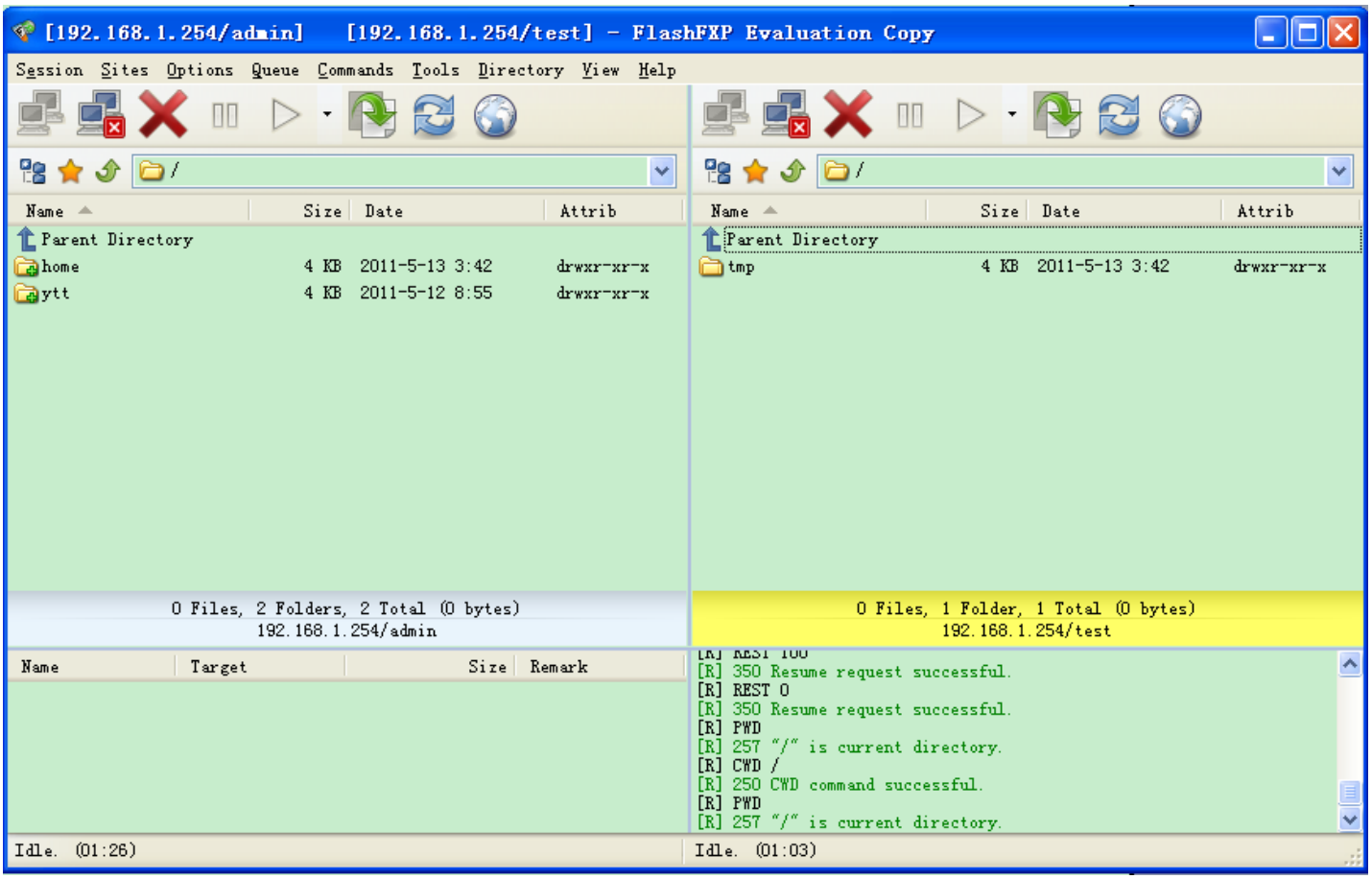
3. Choose the account which you want to edit then you can change the account's parameters, click Edit/Delete to confirm changes.



4. Choose the account which you want to delete, click Edit/Delete to remove it.



In the above example, we add a user named test. And the user is granted with authority of FTP and Samba server access. User test can access the FTP server with FTP access client (first enable FTP server in FTP Server section). Use Samba server, please enable first.


[192.168.1.254/admin] [192.168.1.254/test] - FlashFXP Evaluation Copy
Session Sites Options Queue Commands Tools Directory View Help
Name Size Date Attrib
Parent Directory
home 4 KB 2011-5-13 3:42 drwxr-xr-x
ytt 4 KB 2011-5-12 8:55 drwxr-xr-x
0 Files, 2 Folders, 2 Total (0 bytes)
192.168.1.254/admin
Name Size Date Attrib
Parent Directory
tmp 4 KB 2011-5-13 3:42 drwxr-xr-x
0 Files, 1 Folder, 1 Total (0 bytes)
192.168.1.254/test
Name Target Size Remark
[R] 350 Resume request successful.
[R] REST 0
[R] 350 Resume request successful.
[R] PWD
[R] 257 "/" is current directory.
[R] CWD /
[R] 250 CWD command successful.
[R] PWD
[R] 257 "/" is current directory.
Idle. (01:26)
Idle. (01:03)

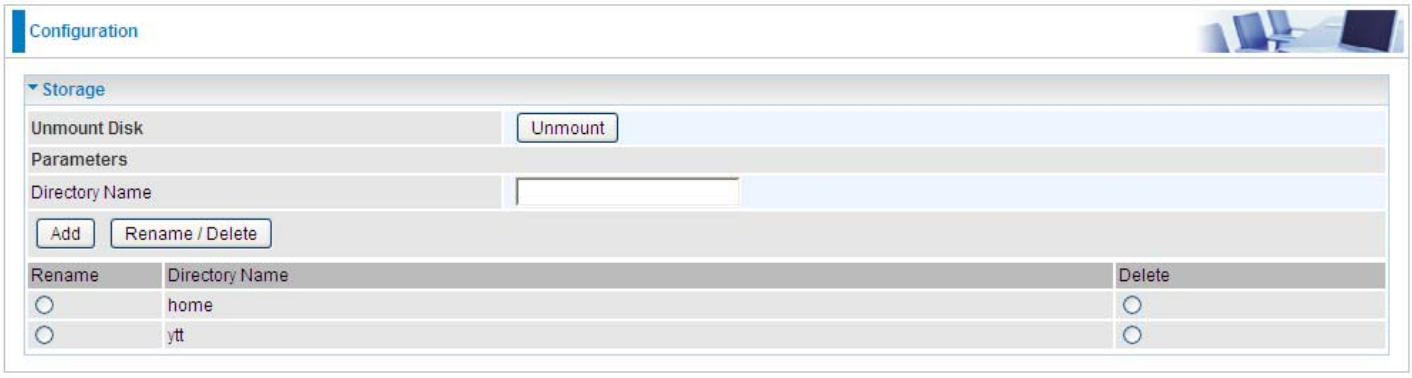
Two ftp sessions with admin and test respectively.

5.3.4.2 Storage

Storage page displays the information of storage device which plugged in USB port.

In the listing, all the folders in the USB device will be shown. For example, in the following diagram, you will Folder home and ytt.

In this section, you can create/delete/rename the folders in the storage device.

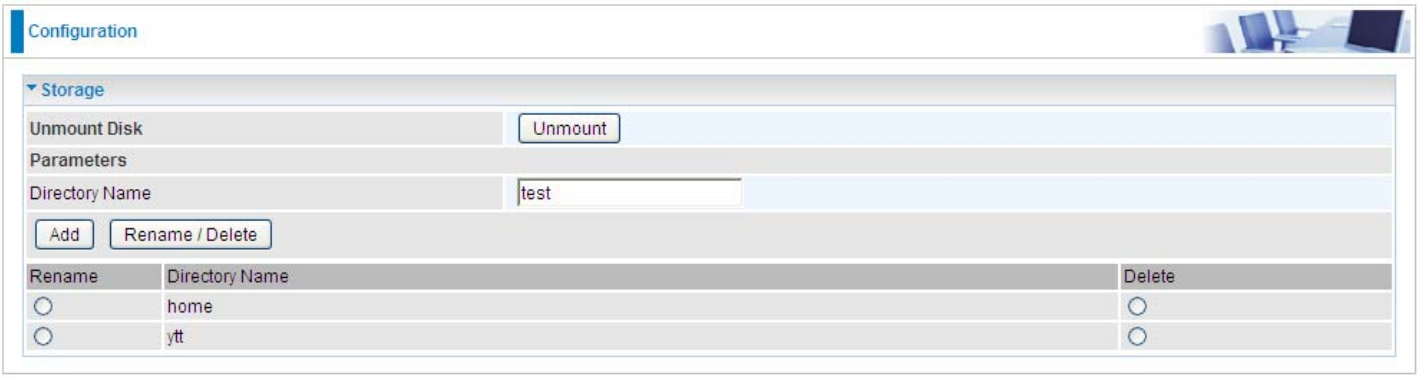


Unmount Disk: Press **Unmmount** button if you want uninstall the USB device, then you can pull out the device.

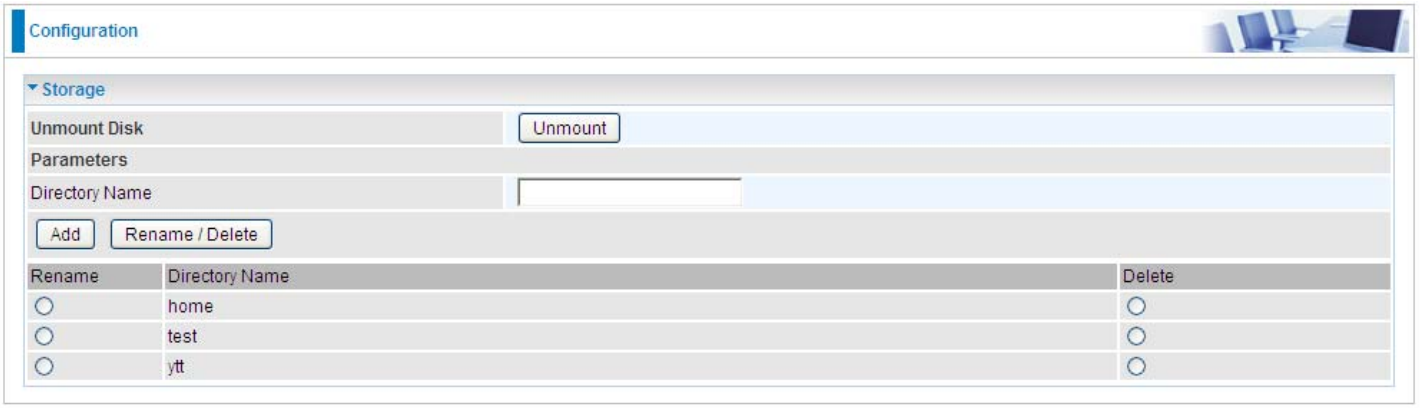
Directory Name Enter the directory name which you wish to create in the Directory Name field.

Add/Delete directory

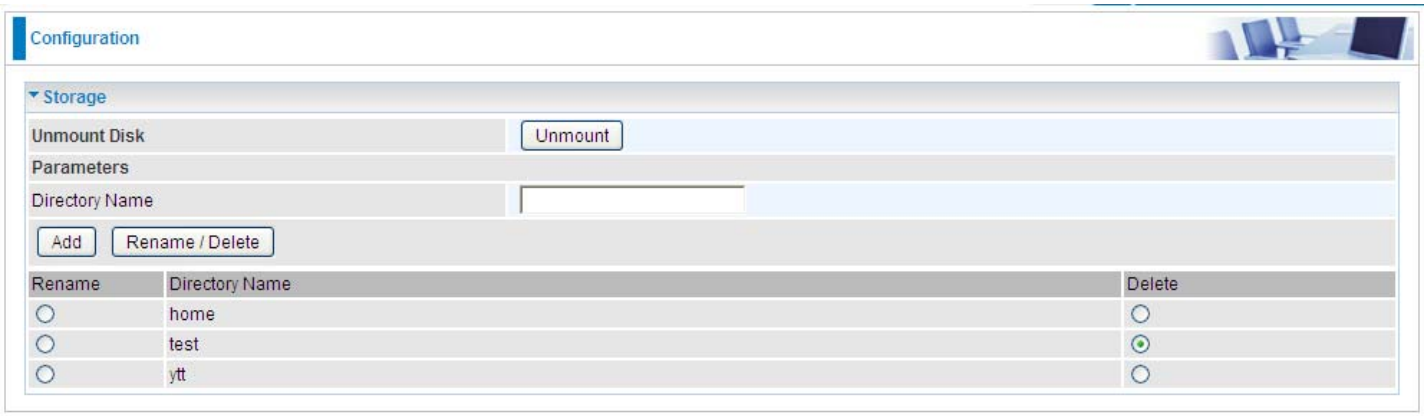
1. Enter directory name in the directory name field and choose partition path which the directory will located.



2. Click **Add**. The New directory will display below.

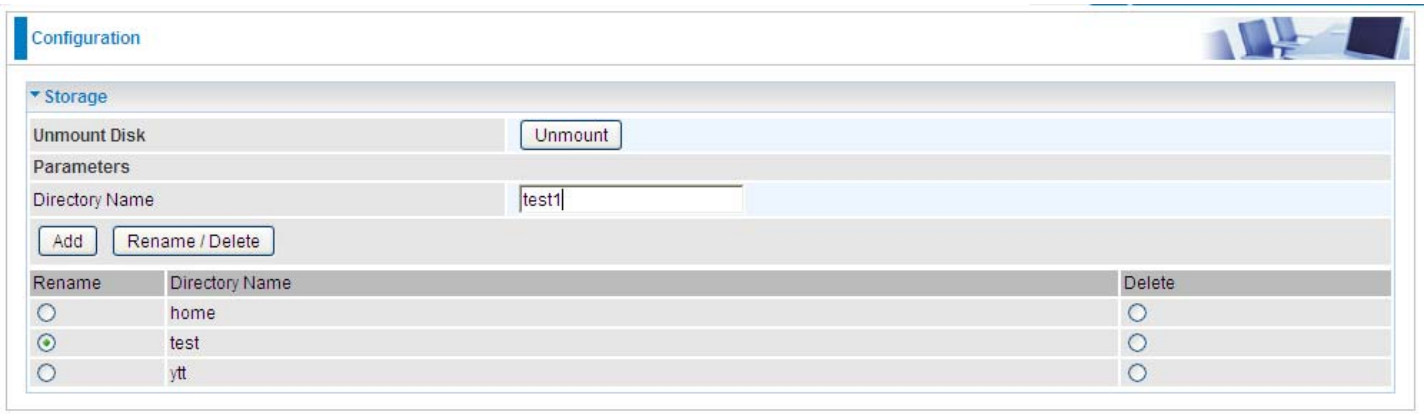


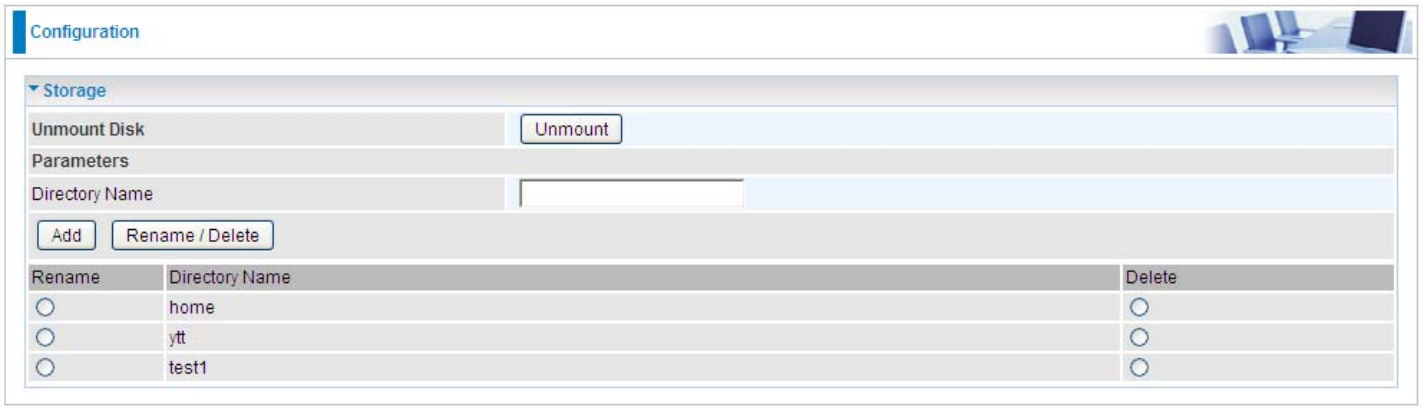
3. Choose the directory which you want to delete then click **Rename/Delete** to romove this directory. A message from webpage will remind you by ”Are you sure to deleter data?” before you decide to submit the command.



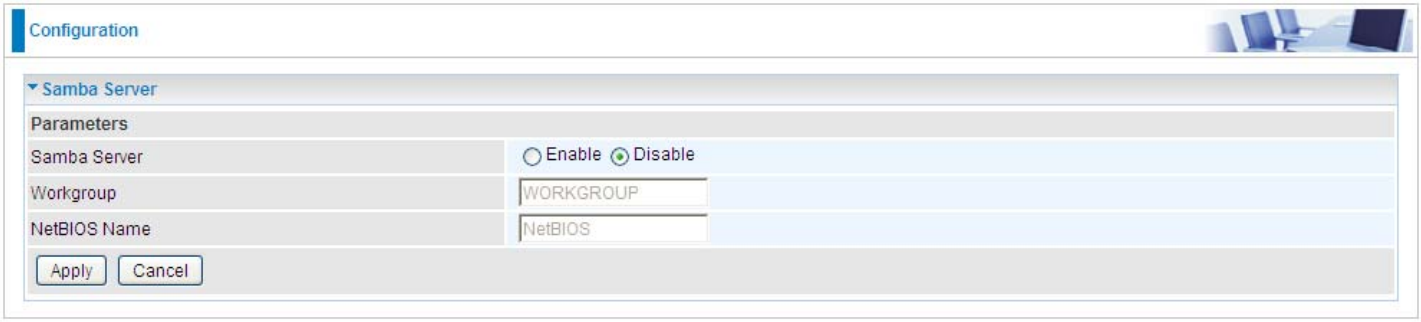
Rename directory

Choose the directory which you want to rename then enter the new name for the folder, and click **Rename/Delete** to rename this directory.

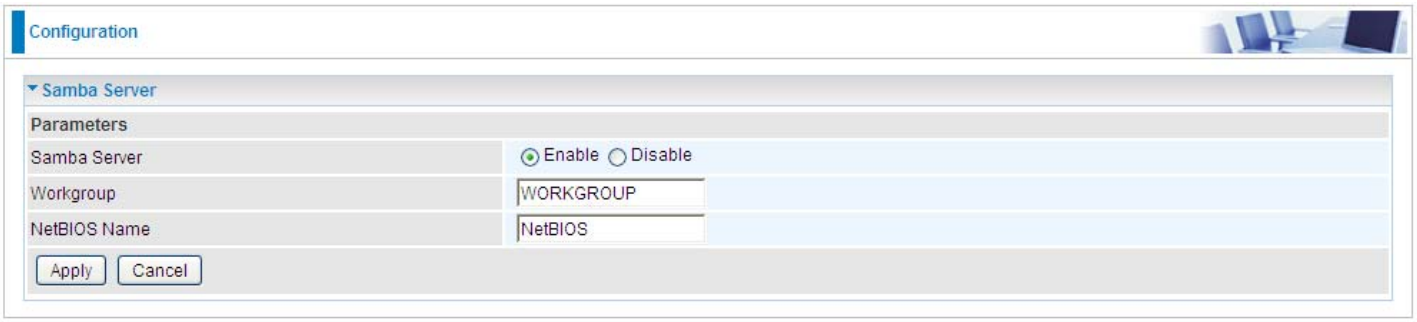




5.3.4.3 Samba Server



Samba Server Setup



Samba Service: Enable or Disable Samba Server function.

Workgroup: Enter the workgroup name in this field which should be same as workgroup name for PCs.

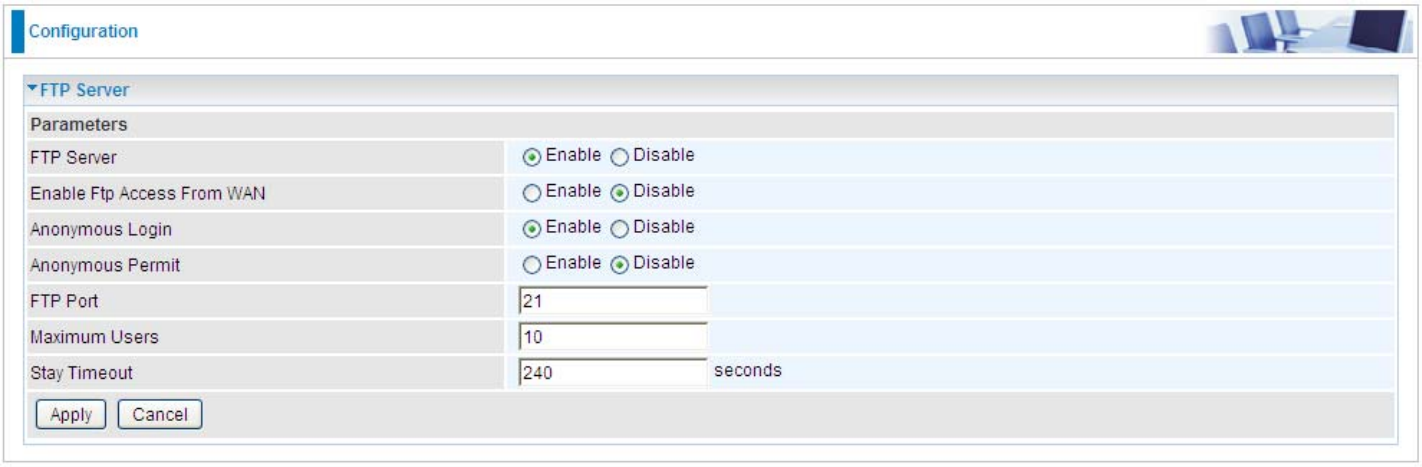
NetBIOS Name: Enter NetBIOS name in this field. In Network Neighborhood, you will find this Samba server name.

Click **Apply** to confirm the configuration.

5.3.4.4 FTP Server

Enable FTP Server feature, your device can serve as a FTP server, you can use FTP access client or windows cmd to upload/download files.

Note: to give access to users, please go to USB > User Management. In User Management section, set the authority for the user.



FTP Server: Enable or Disable FTP Server function.

Enable Ftp Access From WAN: Enable or Disable access FTP Server from WAN. Default setting is set to disable. Enable this function, both WAN and LAN can use FTP server.

Anonymous Login: Enable or disable Anonymous Login. If enabled, user can login with username Anonymous, but note user login with this account can only access files in the /home/temp.

Anonymous Permit: Enable or disable Anonymous Permit. If you enable this function, this will permit the anonymous user to Download/Upload/Create new folder/Delete file. But if disabled, user will only have right to Download/Upload files.

FTP Port: Enter FTP port in this field; please avoid conflicts with other port.

Max. Users: This option specifies the maximum number of user accounts.

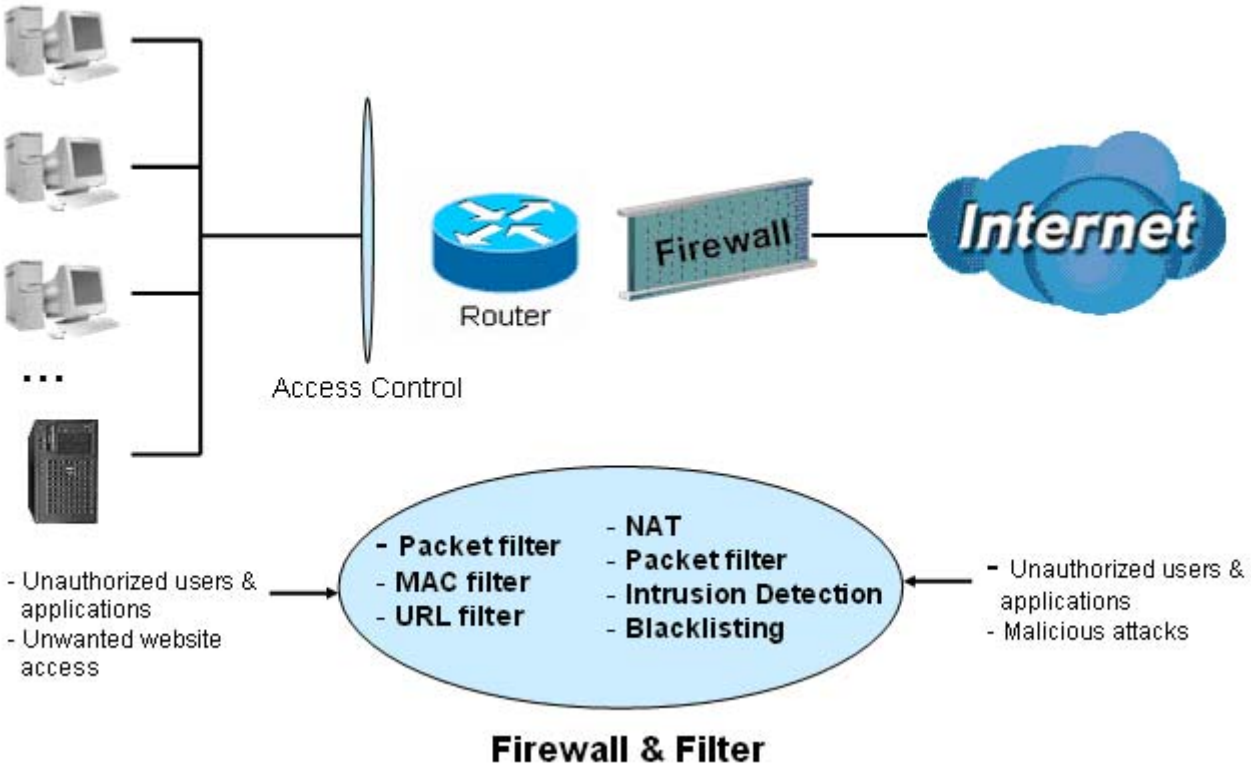
Stay Timeout: Enter the Stay timeout value. Auto-disconnect when there is no activity for a predetermined period of time. The default value is 240 seconds.

Click **Apply** to save the configuration.

5.3.5 Firewall

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall & Filter

Firewall: Prevents access from outside your network.

NAT natural firewall: This masks LAN users’ IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

NOTE:

When using Virtual Servers (port mapping) your PCs are exposed to the ports specified opened in your firewall packet filter settings.

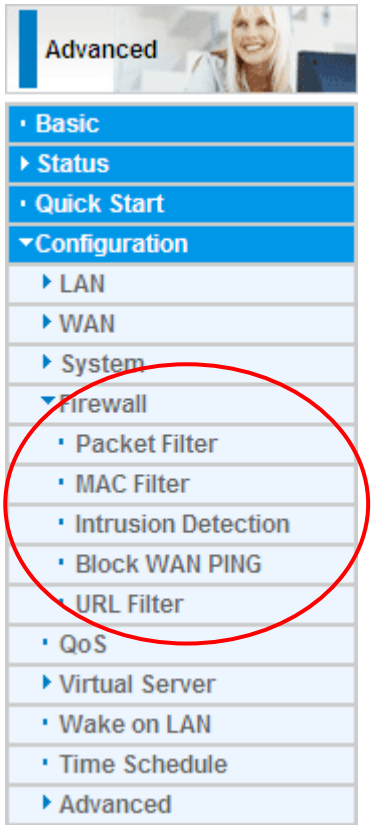
Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent, and log malicious attacks.

MAC Filter rules: Prevents unauthorized computers accessing the Internet.

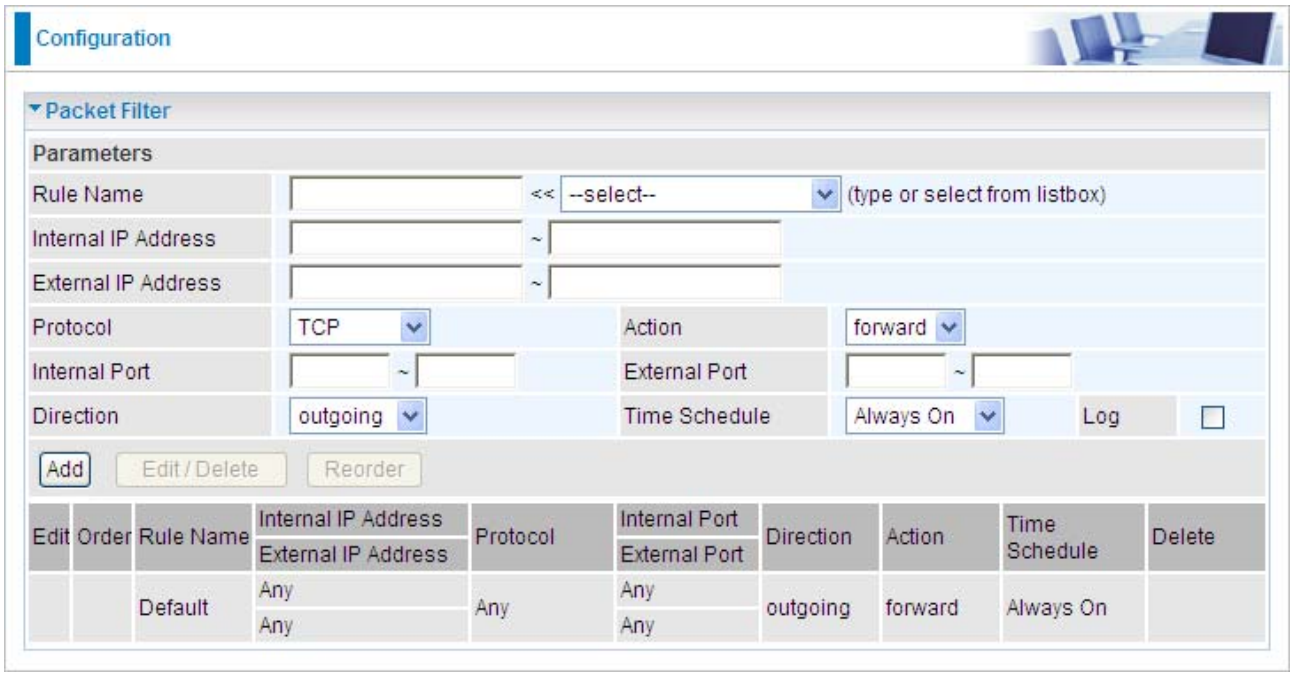
URL Filter: Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following five items appears in the **Firewall** section below: **Packet Filter**, **MAC Address Filter, Intrusion detection, Block WAN PING** and **URL Filter.**



5.3.5.1 Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Rule Name: Users-define description to identify this entry. The maximum name length is 32 characters, and then can choose application that they want from listbox.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Input the range you want to filter out. If you leave empty or 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to.

Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.

Action: If a packet matches this filter rule, **Forward (allows the packets to pass)** or **Drop (disallow the packets to pass)** this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535.** It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

- **Direction:** Determine whether the rule is for outgoing packets or for incoming packets.
- **Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.
- **Log:** Choose “log” if you wish to generate logs when the filer rule is applied to a packet.
- **Add:** Click this button to add a new packet filter rule and the added rule will appear at the bottom table.
- **Edit:** Check the Rule No. you wish to edit, and then click “Edit”.
- Delete: Check the Rule No. you wish to delete, and then click “Delete”.
- **Reorder:** Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press “Reorder” to save the new priority.

Click **Add** to add the item configured and the corresponding information will be listed below just as the following.

Edit	Order	Rule Name	Internal IP Address External IP Address	Protocol	Internal Port External Port	Direction	Action	Time Schedule	Delete
○	↓	FTP	Any Any	TCP	Any 21~21	outgoing	forward	Always On	☐
○	↑	HTTP	Any Any	TCP	Any 80~80	outgoing	forward	Always On	☐
		Default	Any Any	Any	Any Any	outgoing	forward	Always On	

Press **Edit** radio button, the item you want to re-edit will be displayed in the editing area, edit then press **Edit/Delete** to confirm your modification. If you want to delete the rule, check Delete, then press **Edit/Delete** to delete the rule.

Attention

If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

5.3.4.2 MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.

The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Filter Action

Action: Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

Parameters

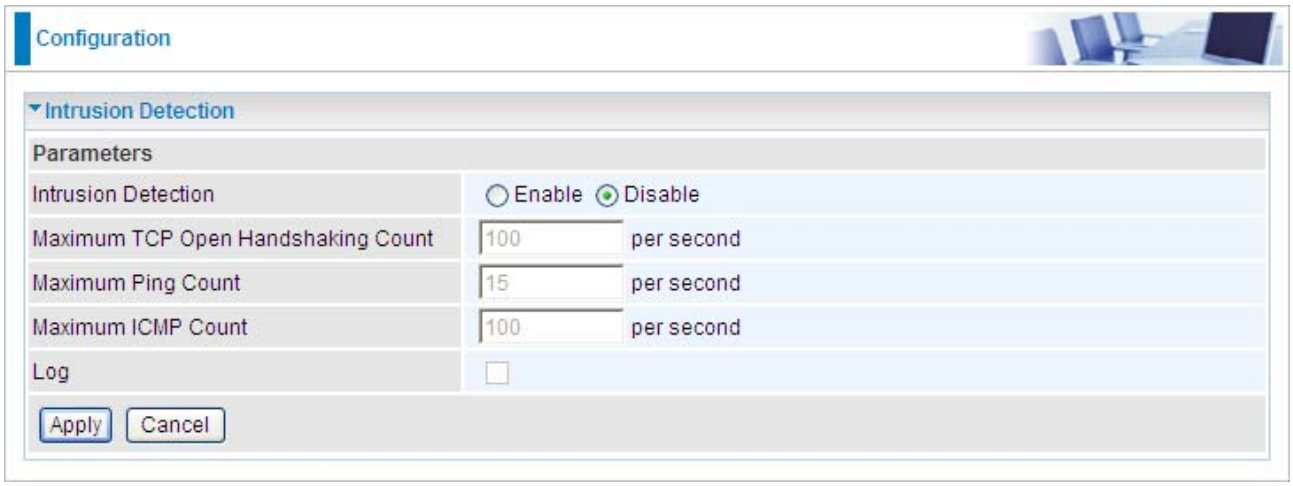
MAC Address: Enter the Ethernet MAC addresses you wish to have the filter rule applies to.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

For Add, Edit, Delete, see the **Packet filter.**

5.3.4.3 Intrusion Detection

Check Enable if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users will have trouble accessing the network resources.



- **Intrusion Detection:** Check Enable if you wish to detect intruders accessing your computer without permission.
- **Maximum TCP Open Handshaking Count:** This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.
- **Maximum Ping Count:** This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.
- **Maximum ICMP Count:** This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).
- **Log:** Check Log if you wish to generate logs when the filer rule is applied to the Intrusion Detection.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log but it will not be able to protect against such attacks.

Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP **Src Port:** Source Port

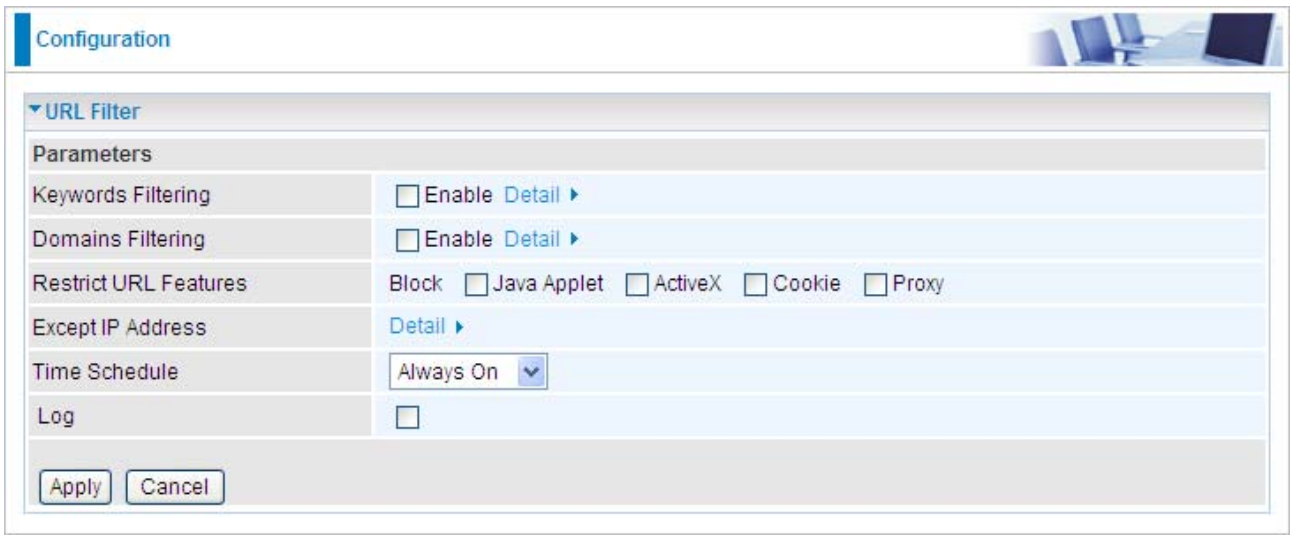
Dst Port: Destination Port Dst IP: Destination IP

5.3.4.4 Block WAN PING

Check Enable if you wish to exclude outside PING requests from reaching this router.

5.3.4.5 URL Filter

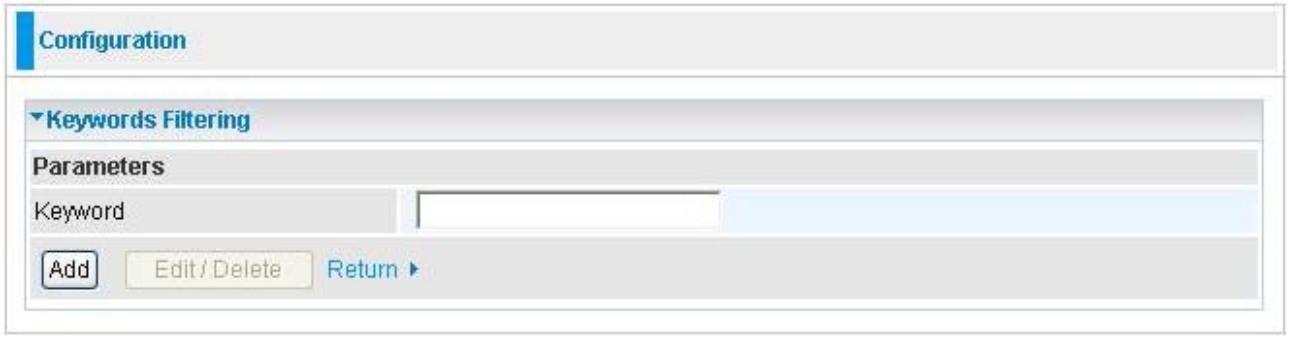
URL (Uniform Resource Locator – e.g. an address in the form of **http://www.example.com**) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

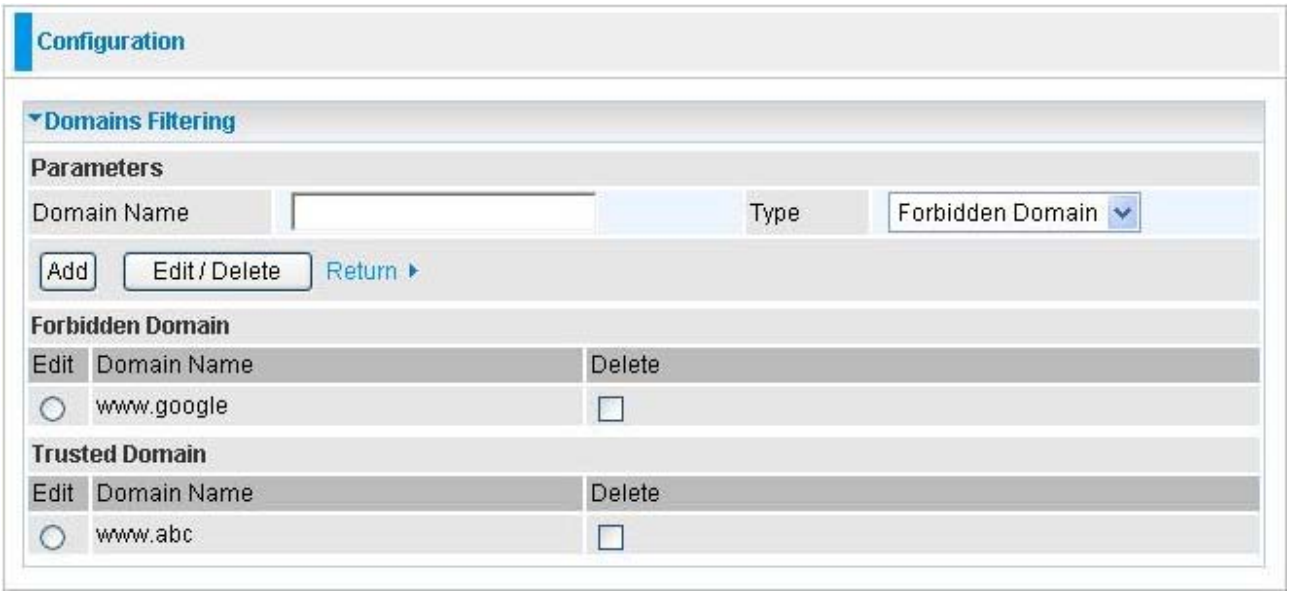
For example, the URL http://www.abc.com/abcde.html would be dropped since the keyword

“abcde” occurs in the URL.



Domains Filtering: Checks the domain name in URLs accessed against your list of domains to block or allow. If it matches, the URL request is sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to www.google.com.au, enter “www.google” or “www.google.com”



Restrict URL Features: This function enhances the restriction to your URL rules.

⊙ **Block Java Applet:** Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.

⊙ Block ActiveX: Blocks ActiveX

⊙ Block Cookies: Blocks Cookies

⊙ Block Proxy: Blocks Proxy

Except IP Address:

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Click “Log” if you wish to generate logs when the filer rule is applied to the URL Filter.

5.3.5 QoS (Quality of Service)

Quality of Service Introduction

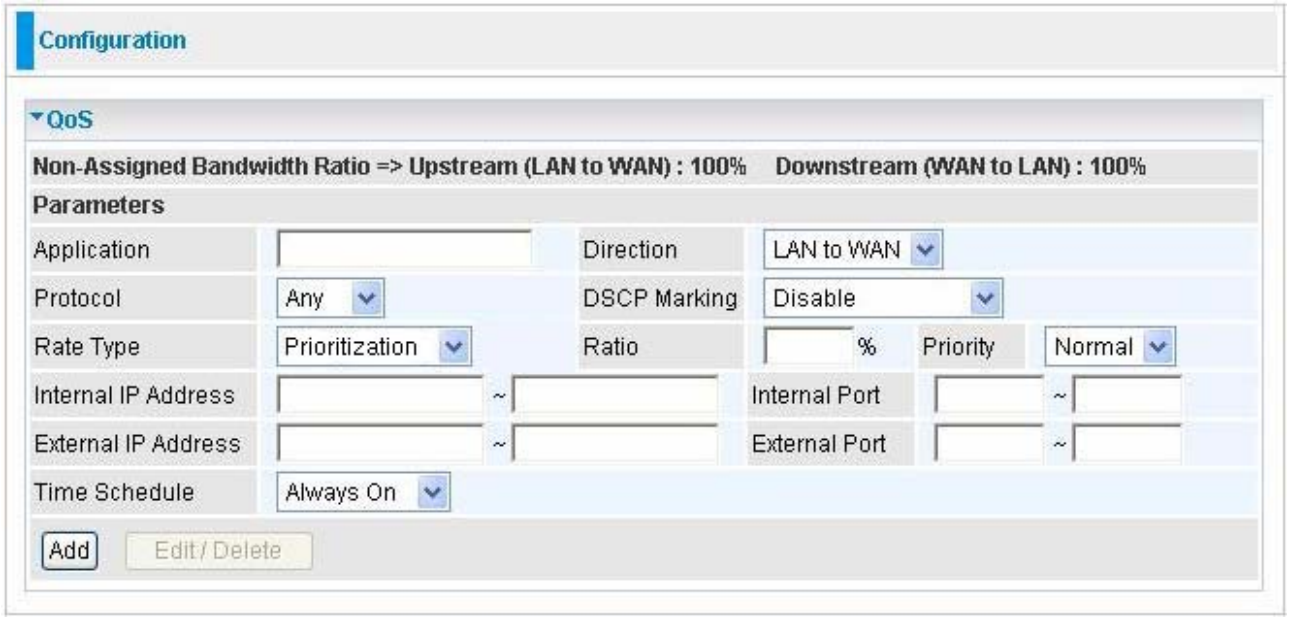
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

QoS: Keeping Your Net Connection Fast and Responsive

Configurable by internal IP address, external IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QoS Setup

Please choose the **QoS** in the **Configuration** item of the left window as depicted below.



After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

- **Application**: A name that identifies an existing policy.
- **Direction**: The traffic flow direction to be controlled by the QoS policy.

There are two settings to be provided in the Router:

⊙ **LAN to WAN:** You want to control the traffic flow from the local network to the outside world (Upstream). You can assign the priority for the application or you can limit the rate your application used. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.

⊙ **WAN to LAN**: Control Traffic flow from the WAN to LAN (Downstream). The connection maybe either issued from LAN to WAN or WAN to LAN.)

Protocol: The Protocol will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

- ⊙ **ANY:** No protocol type is specified.
- ⊙ **TCP**
- ⊙ **UDP**
- ⊙ **ICMP**
- ⊙ **GRE:** For PPTP VPN Connections.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

DSCP Mapping Table	
ADSL2+ Router	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Rate Type: 2 types are provided:

⊙ **Limited (Maximum):** specify a limited data rate for this policy. It also is the maximal rate for this policy. When you choose Limited, type the Ratio proportion. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.

⊙ **Prioritization:** to specify the rate type control for the rule to used. If you choose Prioritization for the rule, you parameter **Priority** would be available, you can set the priority for this rule.

Ratio: Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is 20%*256*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

Priority: Specify the priority for the bandwidth. You can specify which application can

have higher priority to acquire the bandwidth.

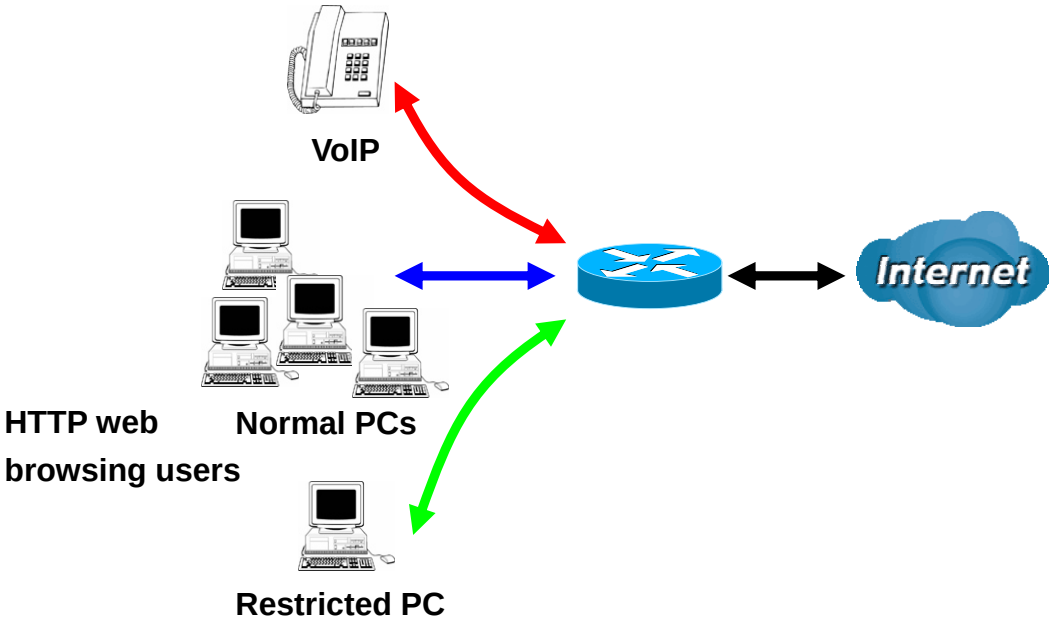
- ⊙ **High**
- ⊙ **Normal**: The default is normal priority.
- ⊙ **Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

- **Internal IP Address:** The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)
- **Internal Port:** The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)
- **External IP Address:** The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)
- **External Ports:** The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)
- **Time Schedule:** Scheduling your prioritization policy.

QoS example for your Network

Connection Diagram



ADSL Subscription Rate

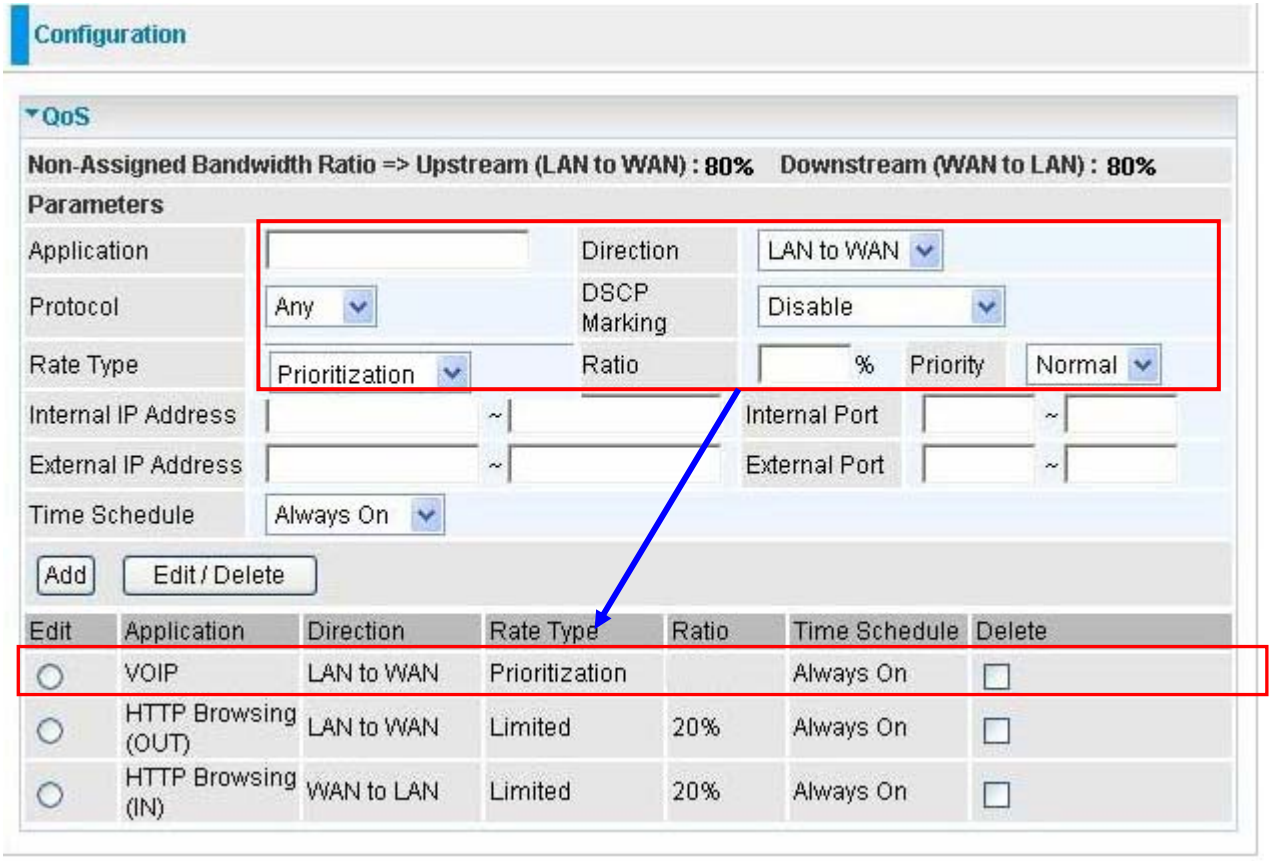
Upstream: 256 kbps

Downstream: 2048 Mbps

Example QoS Plan

Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.1.1	Outgoing	High priority for bandwidth with DSCP marking Class 1 Gold Service.	Always
HTTP web browsing users	80	Incoming and Outgoing	outgoing: limited 20%. Data rate. incoming: limited 20%. Data rate.	Always

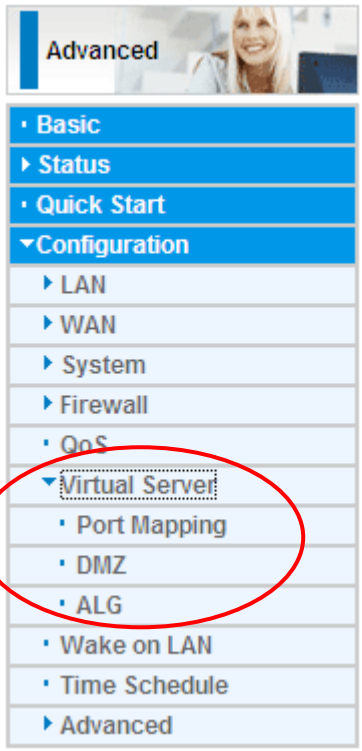
Example QoS Setup



VoIP application

Voice is latency-sensitive application. Most VoIP devices are used SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

5.3.6 Virtual Server



In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are

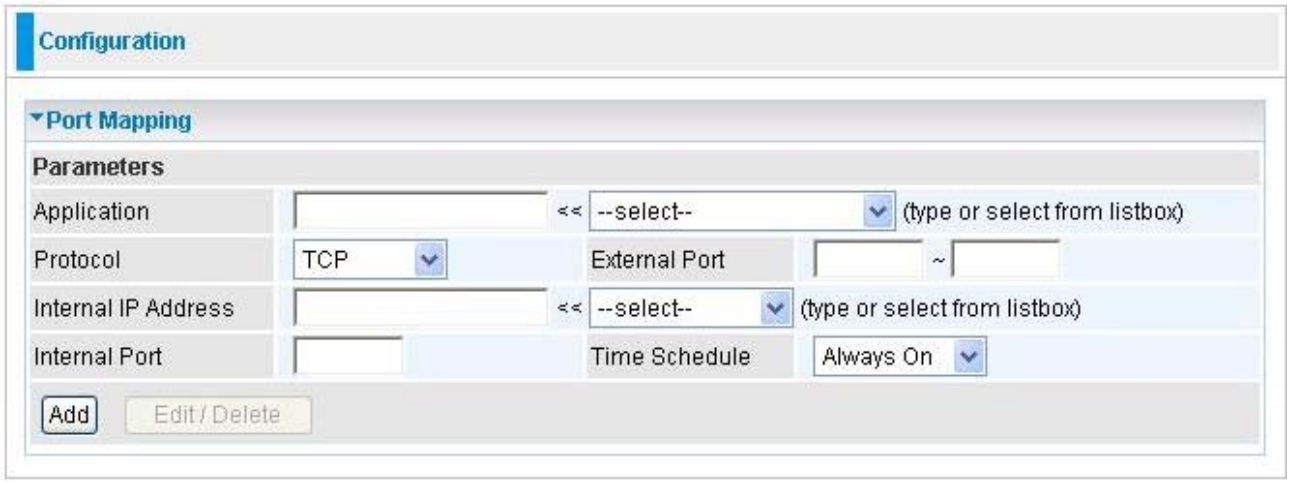
designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	**Protocol**	**Description**
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

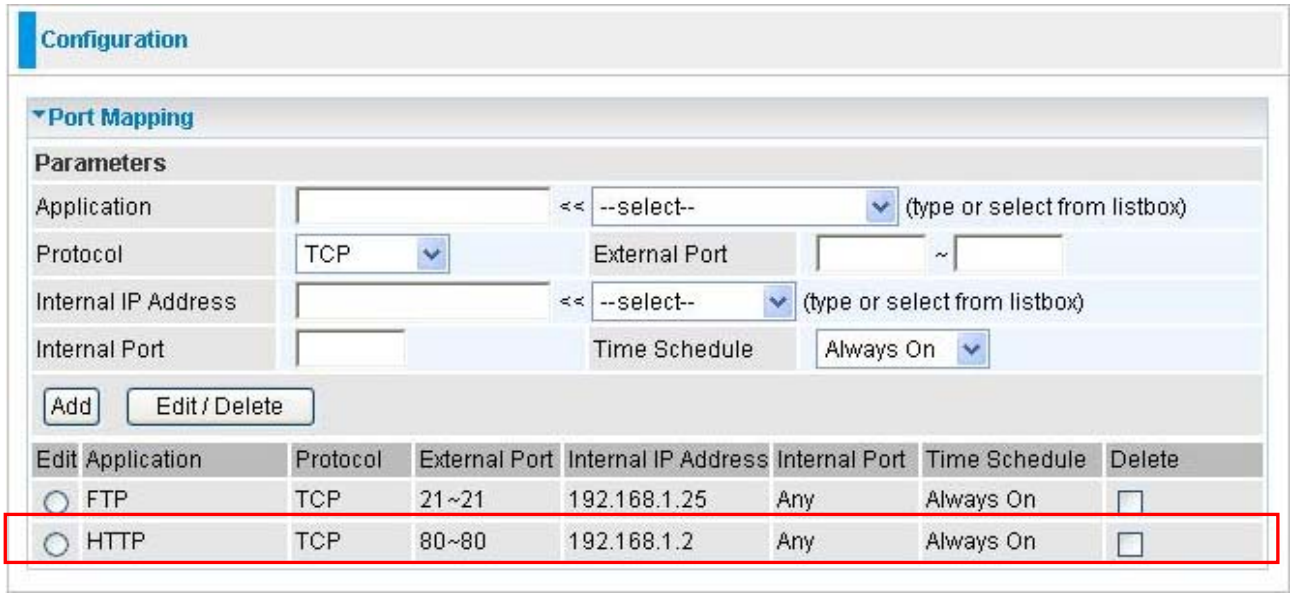
5.3.6.1 Port Mapping



- **Application:** Select the service you wish to configure
- **Protocol:** Automatic when you choose Application from listbox or select a protocol type which you want.
- **External Port & Internal Port:** Enter the public port number & range you wish to configure.
- **Internal IP Address:** Enter the IP address of a specific internal server to which requests from the specified port is forwarded.
- **Add:** Click to add a new virtual server rule. Click again and the next figure appears.
- **Edit:** Check the Rule No. you wish to edit and then click “Edit/Delete”.
- **Delete:** Check the Rule No. you wish to delete then click “Edit/Delete”.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.



In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by the particular application. Most applications use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

5.3.6.2 DMZ

DMZ: The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, it is then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.

5.3.6.3 ALG

Controls enable or disable various protocols over application layer.

For example, SIP ALG:

Enable: When SIP phone need ALG to pass through the NAT.

Disable: When SIP phone included NAT-Traversal algorithm. Turn off the SIP ALG.

NOTE:

Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

Attention

1. If you disable the NAT option in the WAN-ISP section, the Virtual Server function becomes invalid.
2. If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign a static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

5.3.7 Wake on LAN

This feature provides greater flexibility for users to turn on / boot the computer of the network from a remotely site.

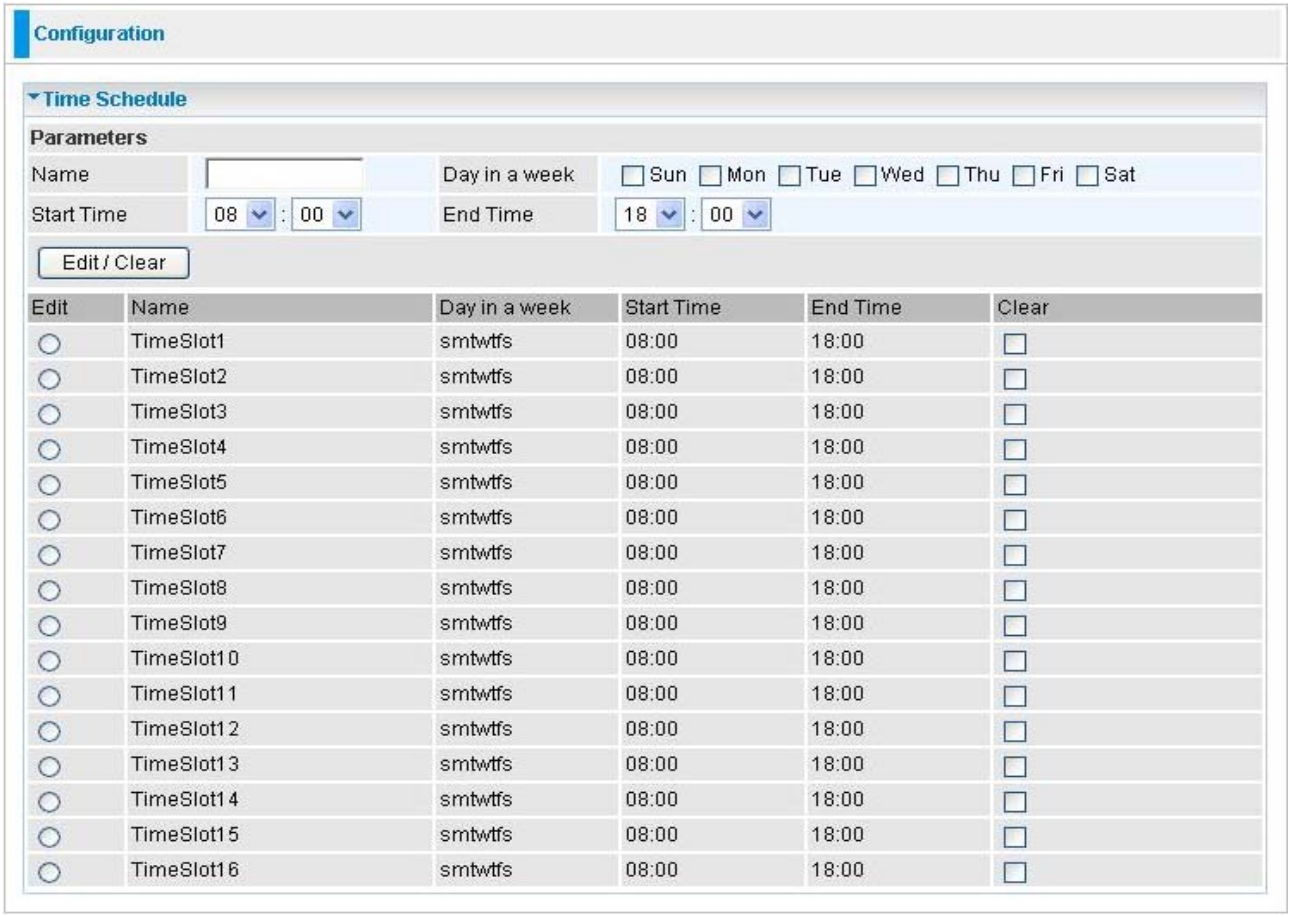
MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the Select drop down menu on the right.

: You can select the MAC from this list.

5.3.8 Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

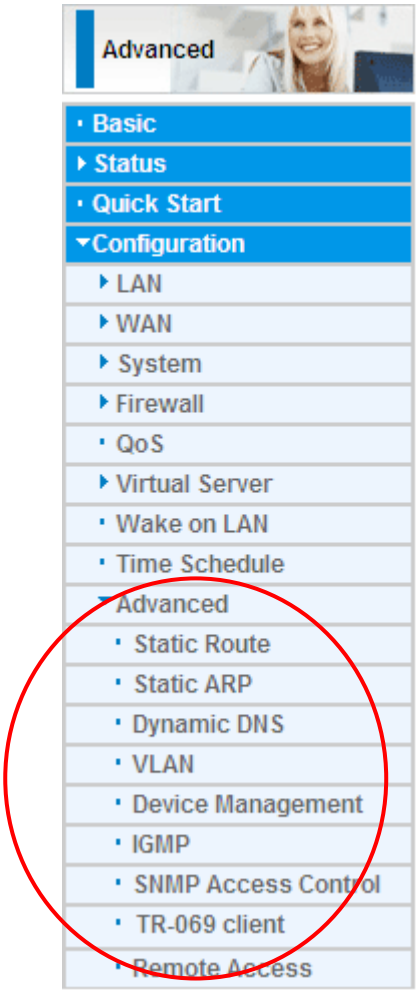


- **Name:** A user-define description to identify this time portfolio.
- **Day in a week:** The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.
- **Start Time:** The default is set at 8:00 AM. You may specify the start time of the schedule.
- **End Time:** The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the **Apply** button to apply your changes.

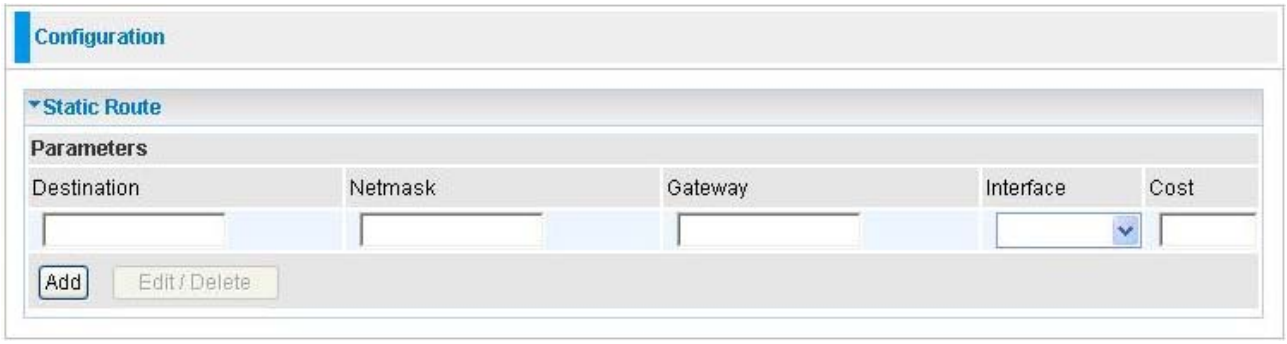
5.3.9 Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are seven items within the **Advanced** section: **Static Route, Static ARP, Dynamic DNS, VLAN, Device Management, IGMP, SNMP Access Control, TR-069 client** and **Remote Access.**



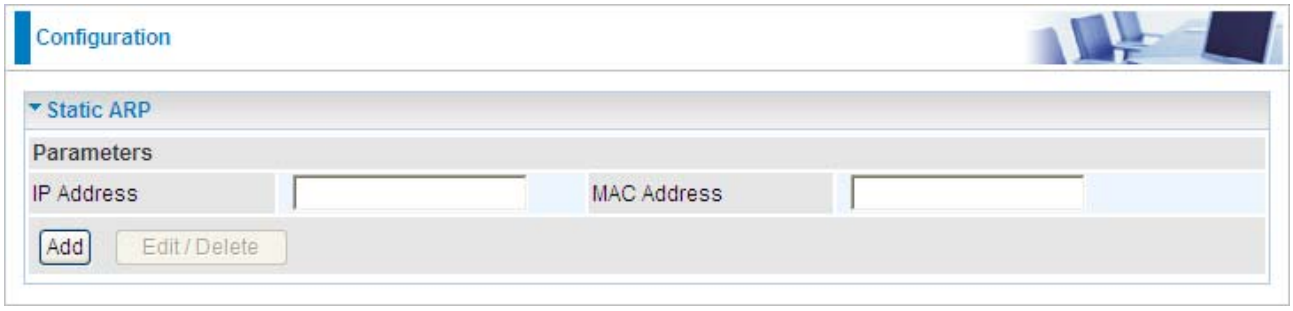
5.3.9.1 Static Route



- **Destination:** The destination subnet IP address.
- **Netmask:** Subnet mask of the destination IP addresses based on above destination.
- **Gateway:** The gateway IP address to which packets are forwarded.
- **Interface:** Select the interface through which packets are forwarded.
- **Cost:** Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

5.3.9.2 Static ARP

This feature allows you to map the layer-2 MAC (Media Access Control) address that corresponds to the layer-3 IP address of the device.

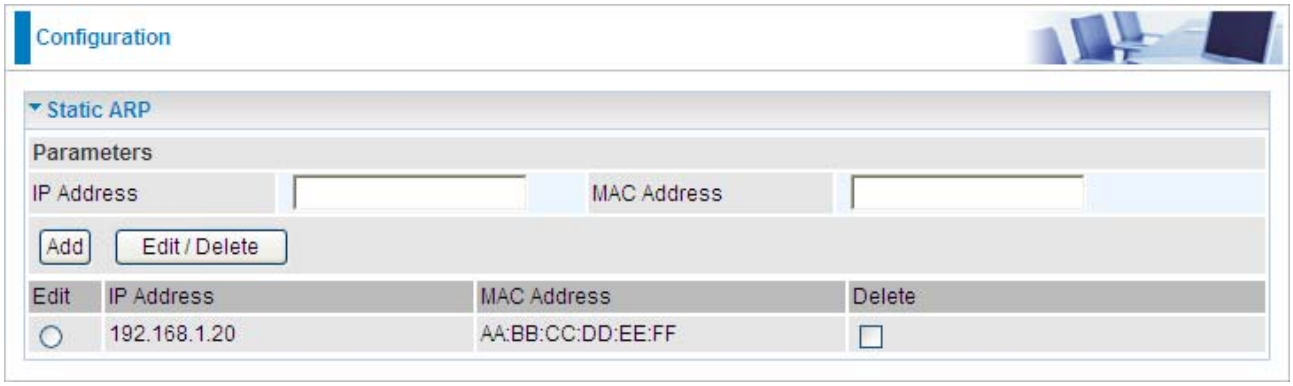


IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.

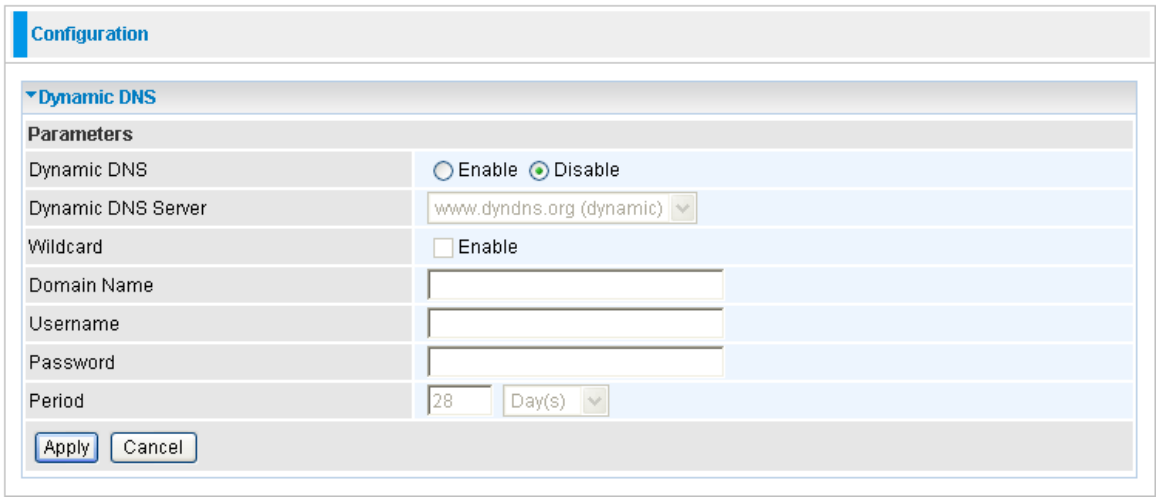


Delete: To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

5.3.9.3 Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You first need to register and establish an account with the Dynamic DNS provider using their web site, for example http://www.dyndns.org/



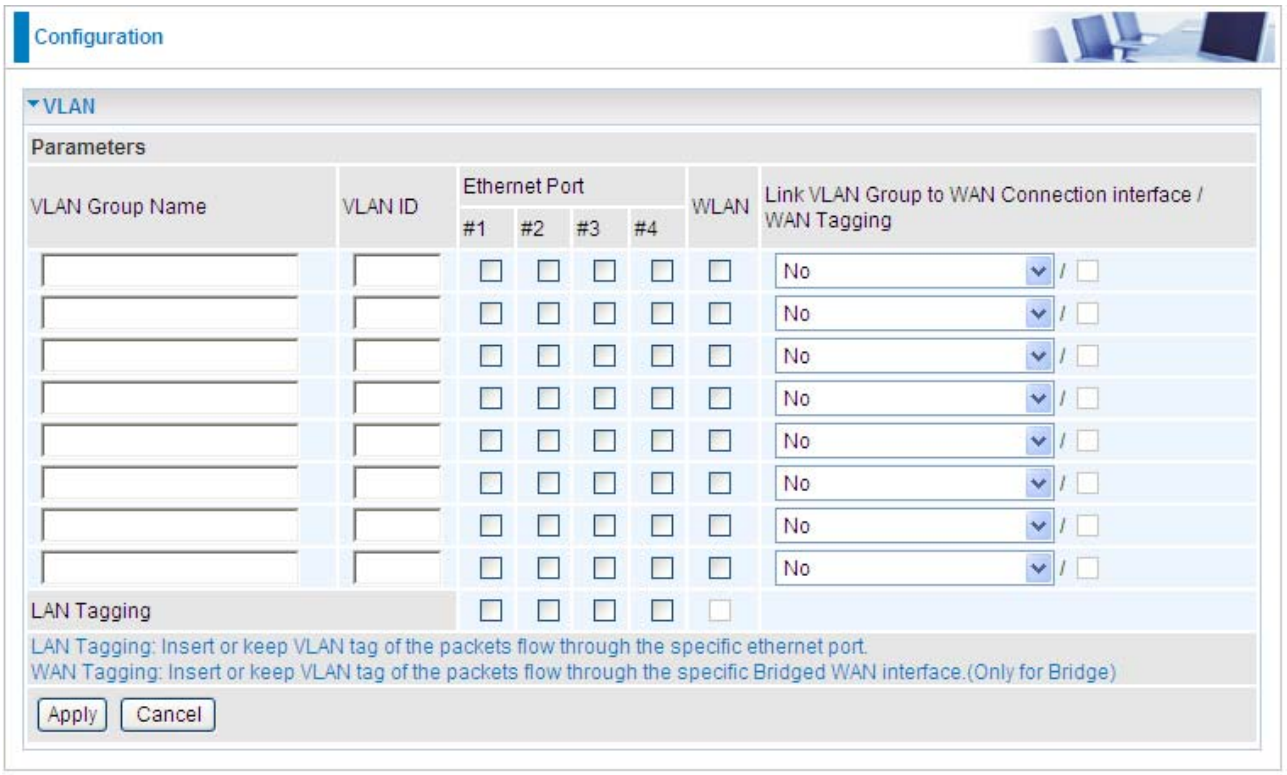
- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The fields following are activated and required.
- **Dynamic DNS Server:** Select the DDNS service you have established an account with.
- **Wildcard:** Select this check box to enable the DYNDNS Wildcard.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes. If the period is 0, the router will check the DNS server every 5 min.

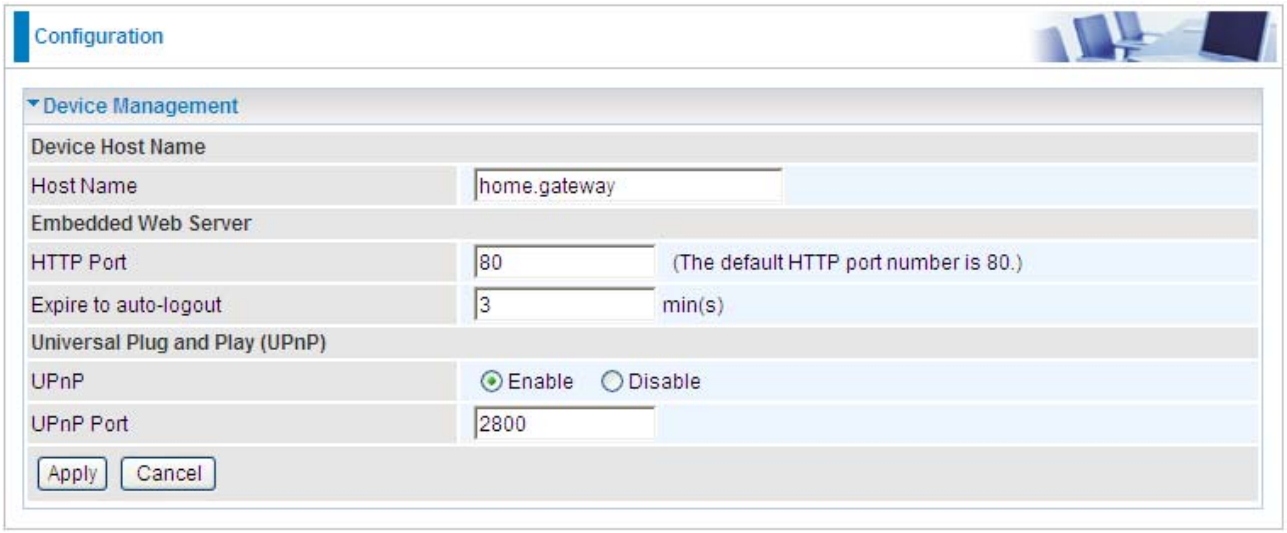
5.3.9.4 VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.



5.3.9.5 Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Embedded Web Server:

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses. The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: **http://192.168.1.254:100** in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

- **Disable:** Check to disable the router's UPnP functionality.
- **Enable:** Check to enable the router's UPnP functionality.
- **UPnP Port:** The Default setting is 2800. It is highly recommended you use this port value. If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows Example

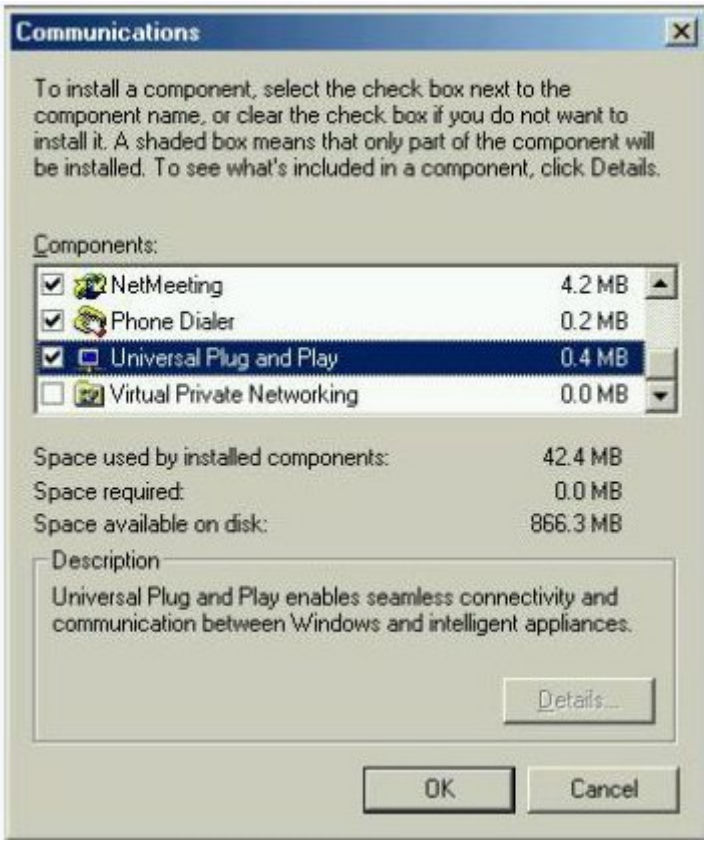
Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessibility 0.0 MB
Accessories 13.8 MB
Address Book 1.5 MB
Communications 7.0 MB
Desktop Themes 5.9 MB
Space used by installed components: 42.8 MB
Space required: 0.0 MB
Space available on disk: 2574.4 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 9 components selected
Details...
Have Disk...
OK
Cancel
Apply

Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

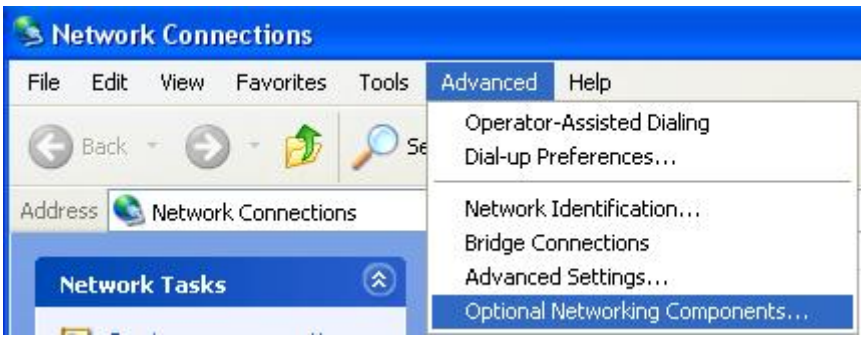
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

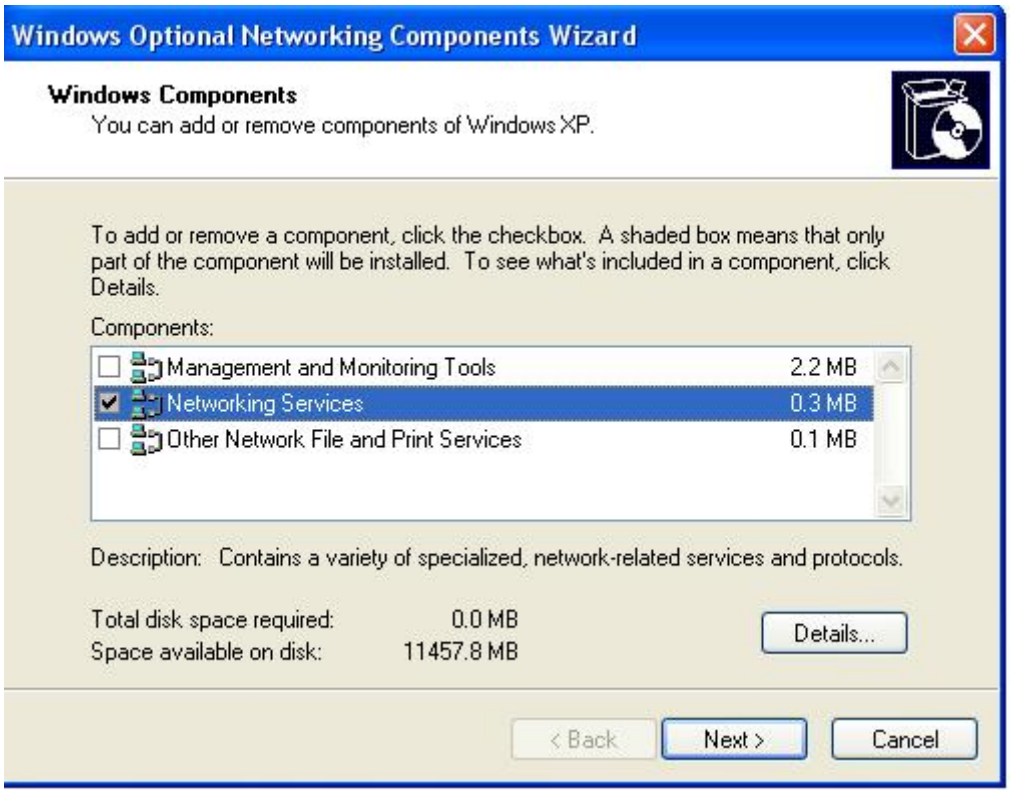
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….



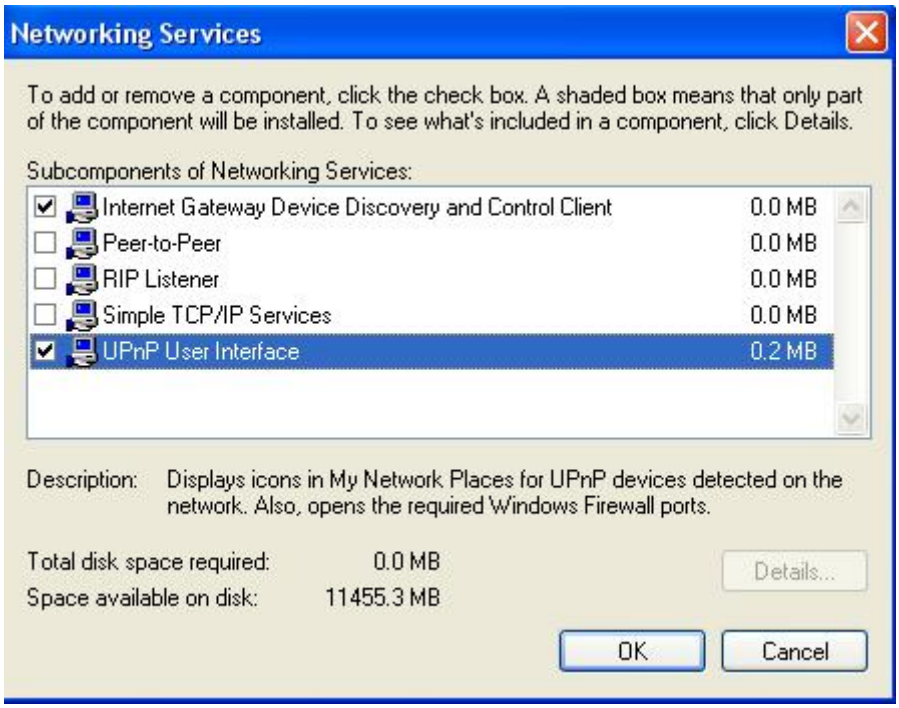
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 2.2 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.1 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 11457.8 MB
Details...
< Back
Next >
Cancel

Step 5: In the Networking Services window, select the Universal Plug and Play check box.

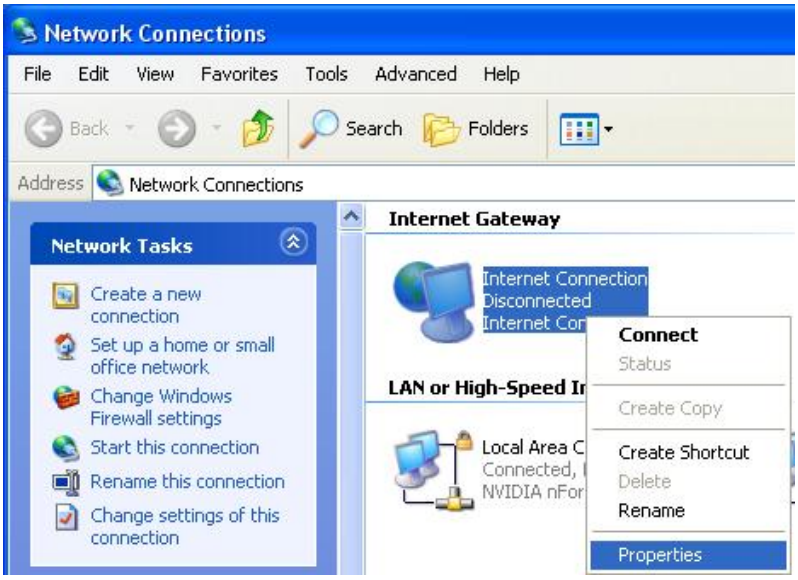
Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.
Total disk space required: 0.0 MB
Space available on disk: 11455.3 MB
Details...
OK
Cancel

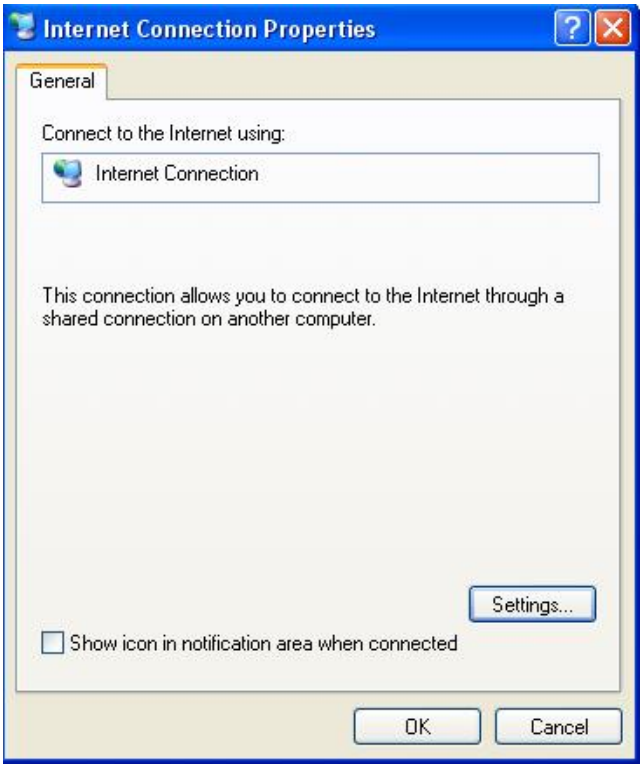
Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

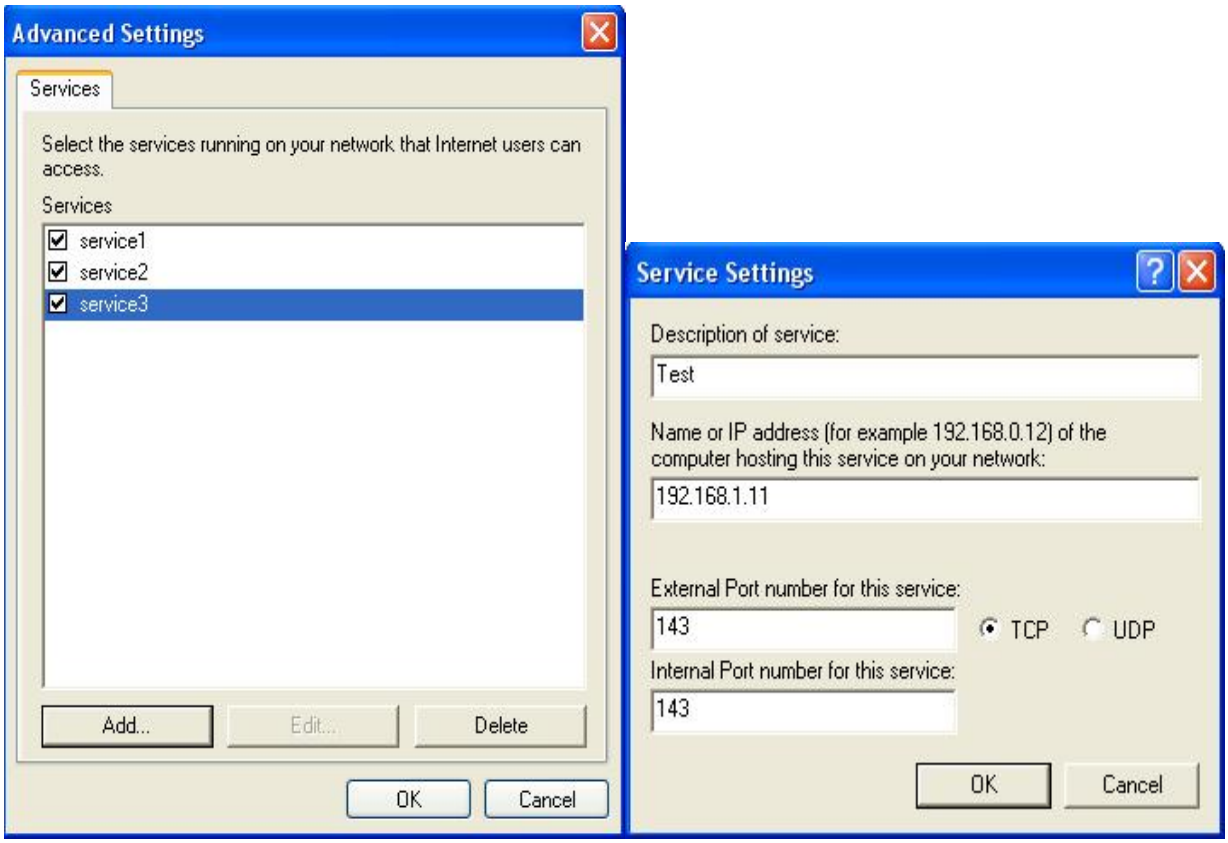
Step 2: Right-click the icon and select Properties.



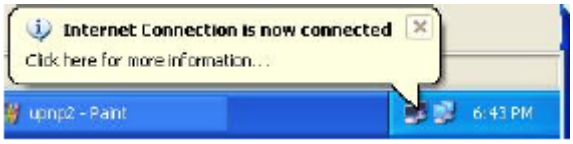
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.


Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

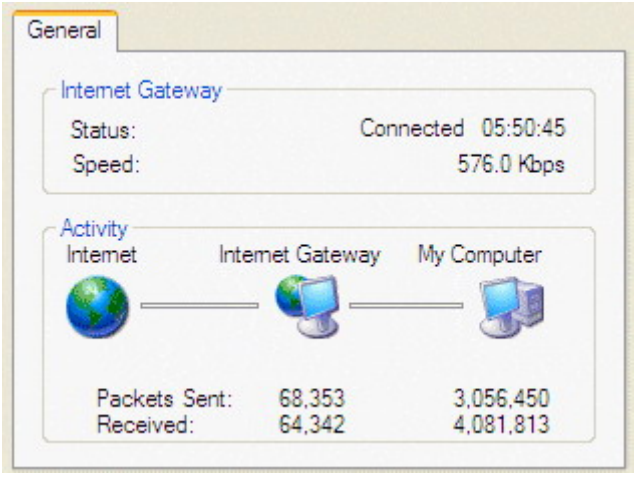
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



Web Configurator Easy Access

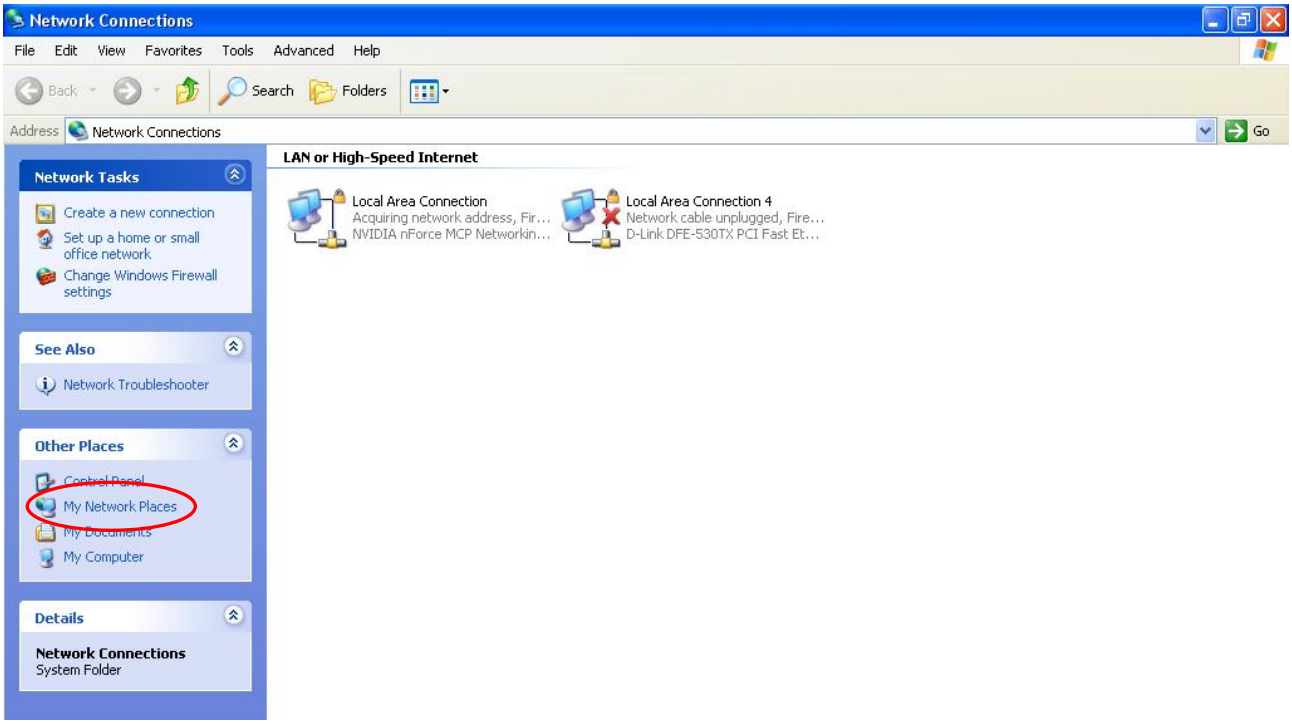
With UPnP, you can access web-based configuration for the BiPAC 7300NX/N *RE* without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 7300NX/N *RE* and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7300NX/N *RE* and select Properties. A properties window displays basic information about the BiPAC 7300NX/N *RE*

5.3.9.6 IGMP

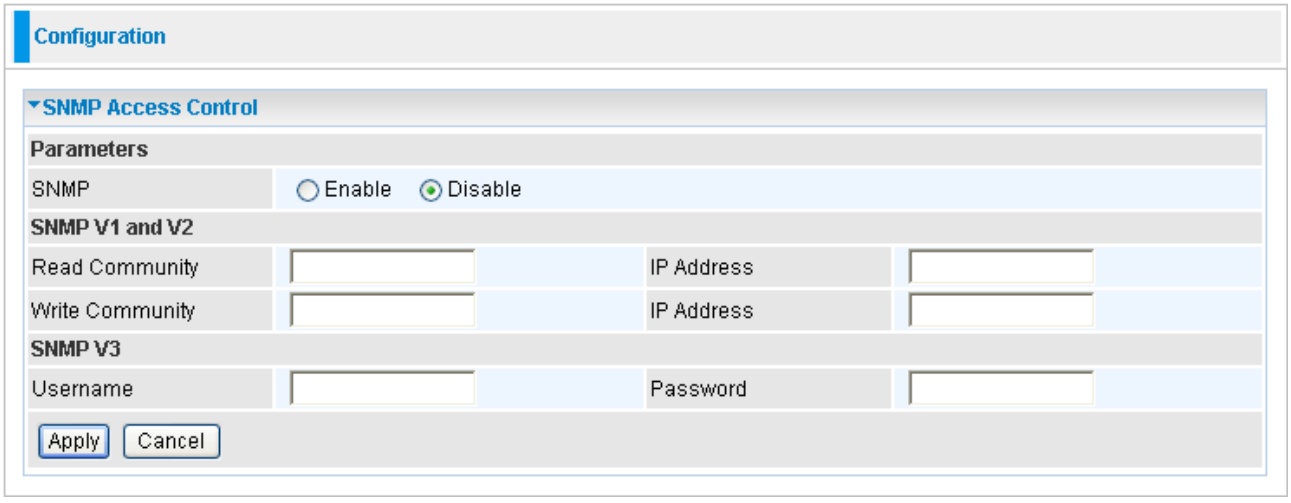
IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.

IGMP Proxy: Accepting multicast packet. Default is set to **Disable.**

IGMP Snooping: Allowing switched Ethernet / Wireless to check and make correct forwarding decisions. Default is set to **Disable.**

5.3.9.7 SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function – Simple Network Management Protocol.



SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to

view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPV2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

☑ System group

☑ Interfaces group

☑ Address Translation group

☑ IP group

☑ ICMP group

☑ TCP group

☑ UDP group

☒ EGP (not applicable)

☑ Transmission

☑ SNMP group

From RFC1650 (EtherLike-MIB):

☑ dot3Stats

From RFC 1493 (Bridge MIB):

☑ dot1dBase group

☑ dot1dTp group

☑ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

☑ pppLink group

☒ pppLqr group

From RFC 1472 (PPP/Security MIB):

☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

☑ PPP Bridge Group

From RFC1573 (IfMIB):

☑ ifMIBObjects Group

From RFC1695 (atmMIB):

☑ atmMIBObjects

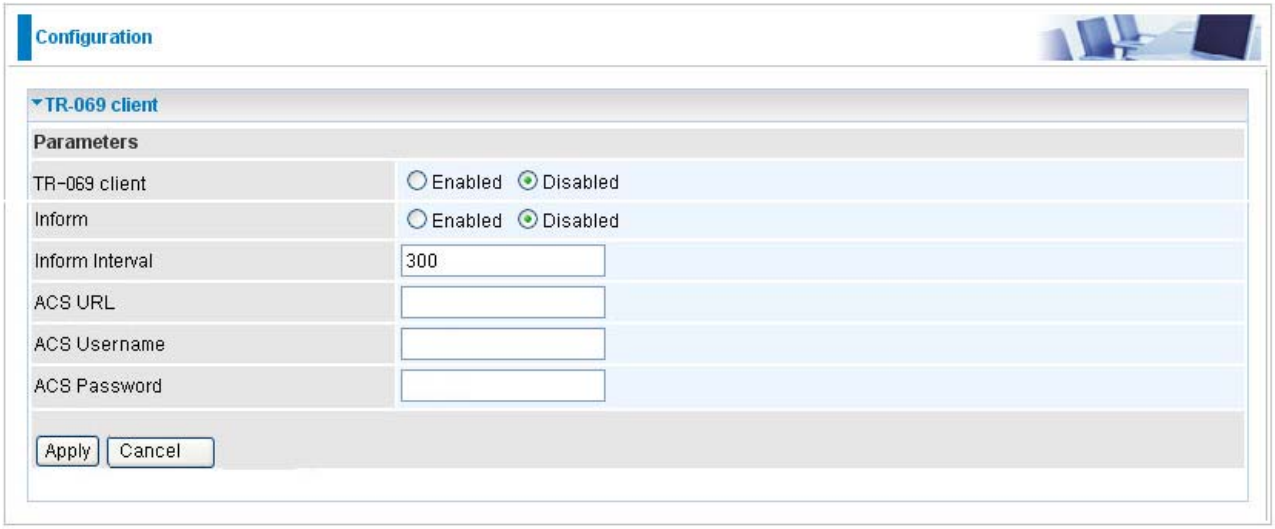
From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

5.3.9.8 TR-069 client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



TR-069 client: select Enable to activate TR-069 client feature.

Inform: select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

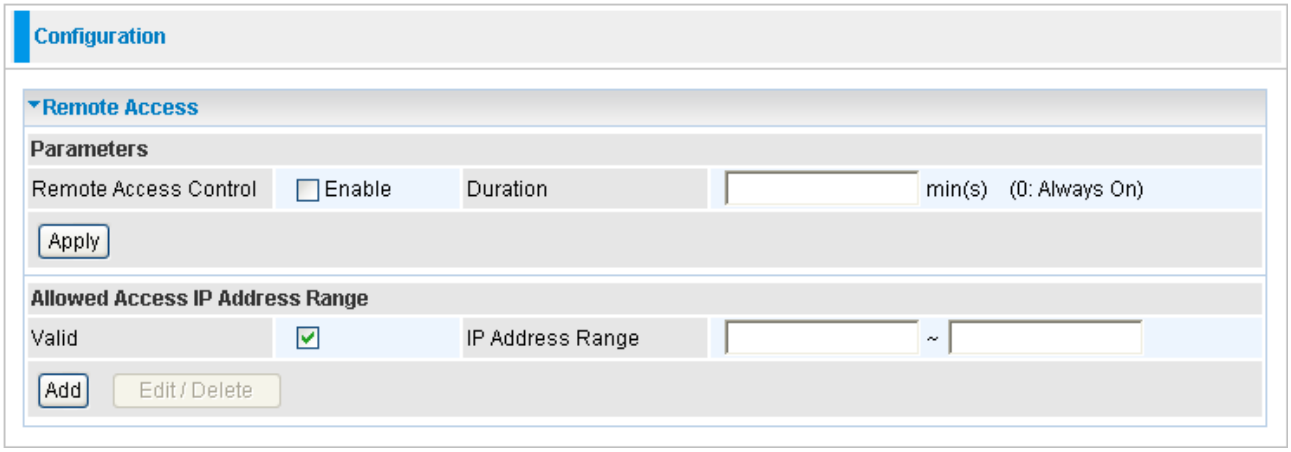
Inform Interval: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

ACS URL: Enter the ACS server login URL.

ACS Username: Specify the ACS User Name for ACS authentication to the connection from CPE.

ACS Password: Enter the ACS server login password.

5.3.9.9 Remote Access



Remote Access Control:

Enable: Select Enable to allow management access from remote side (mostly from internet).

Duration: Set how many minutes to allow management access from remote side. Zero means always on.

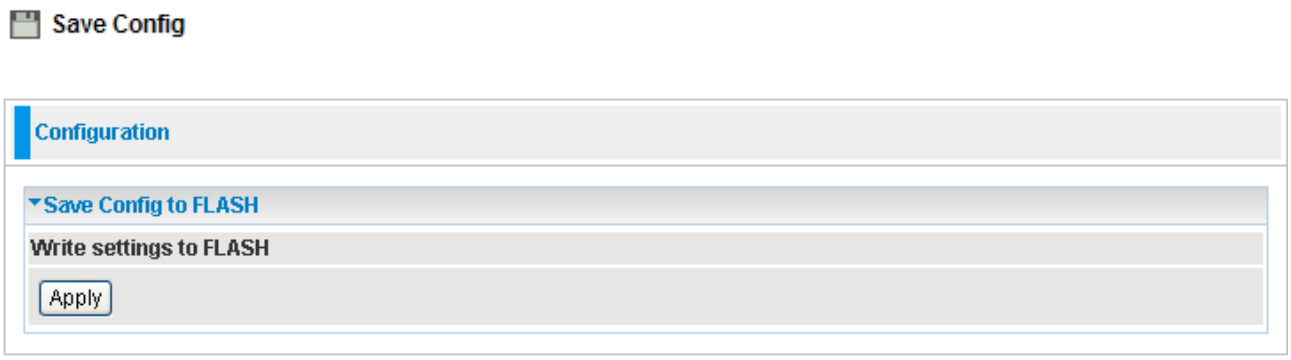
Allowed Access IP Address Range:

Valid: Select Valid to allow remote management from these IP ranges.

IP Address Range: Specify what ip address to be allowed to access device from remote side. Clink Add to insert management ip address list.

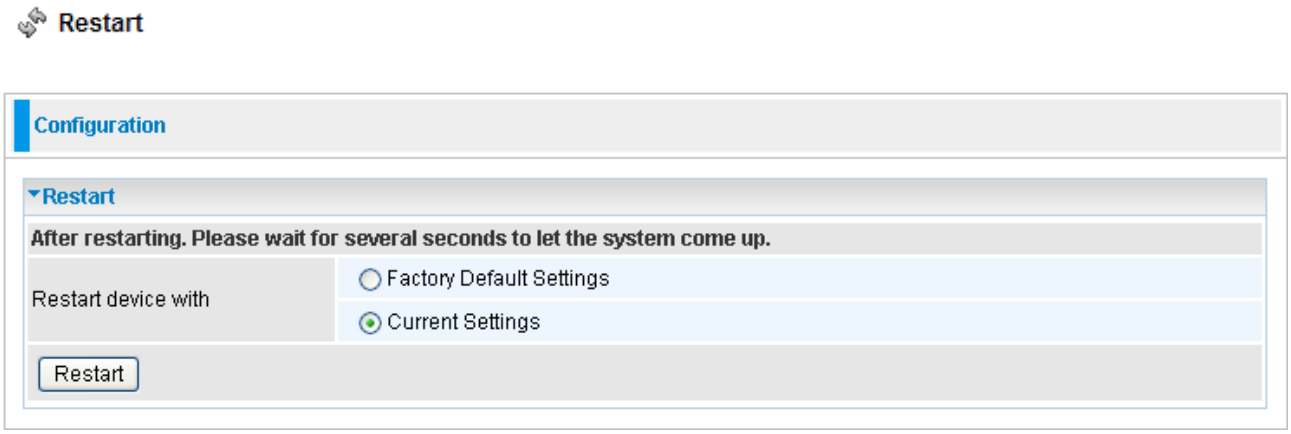
5.4 Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "**Save Config**" and click "**Apply**" to write your new configuration to FLASH.



5.5 Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

5.6 Logout

To exit the router’s web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 6
Troubleshooting

If your ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection ("linesync") failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router. If you still have problems, you may need to verify these settings with your ISP.

Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting. Verify that the IP address and the subnet mask are consistent between the router and the workstations.

APPENDIX

Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

WORLDWIDE

http://www.billion.com

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.